

P23974.P04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Takafumi UENO

Serial No. : Not Yet Assigned

Filed : Concurrently Herewith

For : TRANSMISSION APPARATUS AND RECEIVING APPARATUS


CLAIM OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application No. 2002-210727, filed July 19, 2002. As required by 37 C.F.R. 1.55, a certified copy of the Japanese application is being submitted herewith.

Respectfully submitted,
Takafumi UENO


Bruce H. Bernstein
Reg. No. 29,027

Reg. No.
33,329

July 16, 2003
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2002年 7月19日

出願番号
Application Number:

特願2002-210727

[ST.10/C]:

[JP 2002-210727]

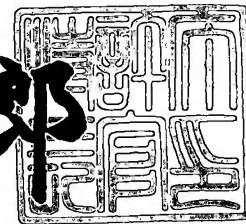
出願人
Applicant(s):

松下電器産業株式会社

2003年 6月16日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3046895



【書類名】 特許願

【整理番号】 2054041179

【提出日】 平成14年 7月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 上野 孝文

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100097445

 【弁理士】

 【氏名又は名称】 岩橋 文雄

【選任した代理人】

 【識別番号】 100103355

 【弁理士】

 【氏名又は名称】 坂口 智康

【選任した代理人】

 【識別番号】 100109667

 【弁理士】

 【氏名又は名称】 内藤 浩樹

【手数料の表示】

 【予納台帳番号】 011305

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 送信装置、及び受信装置

【特許請求の範囲】

【請求項 1】 データを暗号化して第 1 の暗号化データを生成する暗号化手段と、

第 1 の暗号化データと第 1 の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第 1 の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第 1 の暗号化データと前記プログラム仕様情報と前記ツールリストと前記制御グラフと前記権利情報とを多重化する多重化手段とを有する送信装置。

【請求項 2】 データを暗号化して第 1 の暗号化データを生成する暗号化手段と、

第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第 1 の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第 1 の暗号化データと第 1 の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第 1 の暗号化データと前記プログラム仕様情報とを多重化する多重化手段とを有する送信装置。

【請求項 3】 データを暗号化して第 1 の暗号化データを生成する暗号化手段と、

第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリ

ストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

前記データに付随する権利情報を生成する権利情報生成手段と、

前記権利情報を出力する権利情報送信手段と、

第1の暗号化データと前記プログラム仕様情報とを多重化して出力する多重化手段とを有する送信装置。

【請求項4】 前記権利情報と前記データとの対応付けを行う前記権利情報送信手段を有する請求項3に記載の送信装置。

【請求項5】 前記権利情報と前記データとの対応付けを行う前記プログラム仕様情報生成手段を有する請求項3に記載の送信装置。

【請求項6】 暗号を復号する復号ツールを多重化する前記多重化手段を有する請求項1乃至請求項5いずれかに記載の送信装置。

【請求項7】 暗号を復号するための鍵情報を多重化する前記多重化手段を有する請求項1乃至請求項6いずれかに記載の送信装置。

【請求項8】 第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記多重化信号から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、

前記多重化信号から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記多重化信号から第1の暗号化データに付随する権利情報を分離する権利情報手段と、

前記ツールリストから取得したツールIDに従ってツールを入手し、前記制御グラフに従って前記ツールを組み込む第1の制御手段と、

前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを

有する受信装置。

【請求項 9】 第 1 の暗号化データを含む多重化信号を少なくとも第 1 の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記プログラム仕様情報から第 1 の暗号化データに付随する権利情報を分離する権利情報手段と、

前記ツールリストから取得したツール ID を有するツールを前記制御グラフに従って組み込む第 1 の制御手段と、

前記権利情報に従って第 1 の暗号化データを処理する第 1 の権利管理手段とを有する受信装置。

【請求項 1 0】 第 1 の暗号化データを含む多重化信号を少なくとも第 1 の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記ツールリストから取得したツール ID を有するツールを前記制御グラフに従って組み込む第 1 の制御手段と、

第 1 の暗号化データに付随する権利情報を受信する権利情報受信手段と、

前記権利情報に従って第 1 の暗号化データを処理する第 1 の権利管理手段とを有する受信装置。

【請求項 1 1】 受信した第 1 の暗号化データを一時的に記憶する一時記憶手段と、

前記一時記憶手段に記憶された第 1 の暗号化データを読み取る読み取り手段を有する請求項 8 乃至請求項 1 0 いずれかに記載の受信装置。

【請求項 1 2】 前記権利情報に記述された再生許諾が満了した後に第 1 の暗

号化データを前記一時記憶手段から消去するファイル管理手段を有する請求項 1 1 に記載の受信装置。

【請求項 1 3】 第 1 の暗号化データの処理状態を示す状態情報を送信する前記権利管理手段を有する請求項 8 乃至請求項 1 2 いずれかに記載の受信装置。

【請求項 1 4】 前記権利情報を第 1 の権利情報と第 2 の権利情報とに分割する権利管理手段と、

前記多重化信号のうちの前記権利情報を第 2 の権利情報に書き換えて修正多重化信号を出力する多重化修正手段と、

第 2 の受信装置からの要求信号に応じて前記修正多重化信号を第 2 の受信装置に出力する請求項 8 乃至請求項 1 3 に記載の受信装置。

【請求項 1 5】 前記権利情報を第 1 の権利情報と第 2 の権利情報とに分割する権利管理手段と、

第 2 の受信装置からの要求信号に応じて第 2 の権利情報と前記多重化信号を第 2 の受信装置に出力する請求項 8 乃至請求項 1 3 いずれかに記載の受信装置。

【請求項 1 6】 前記権利管理手段は第 2 の受信装置における第 1 の暗号化データの処理状態を示すデータを受信し自身と第 2 の受信装置の処理状態を示す状態情報を送信することを特徴とする請求項 8 乃至請求項 1 5 いずれかに記載の受信装置。

【請求項 1 7】 第 1 の暗号化データを第 2 の暗号化データに変換する変換手段と、

第 2 の暗号化データを第 2 の権利情報とともに再多重化する再多重化手段を有する請求項 8 乃至請求項 1 6 いずれかに記載の受信装置。

【請求項 1 8】 第 1 の権利情報によって第 1 の暗号化データを処理する請求項 8 乃至請求項 1 7 いずれかに記載の受信装置。

【請求項 1 9】 第 1 の暗号化データを第 2 の受信手段に転送後、前記第 1 の暗号化データを前記一次記憶手段から消去するファイル管理手段を有する請求項 1 4 乃至請求項 1 8 いずれかに記載の受信装置。

【請求項 2 0】 前記多重化信号からビデオデータを抽出し復号するビデオ復号手段を有する請求項 8 乃至請求項 1 9 いずれかに記載の受信装置。

【請求項 2 1】 前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する請求項 8 乃至請求項 1 9 いずれかに記載の受信装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、画像圧縮された動画と番組情報を多重化したデジタル放送信号を送信する装置、及び受信する装置に関するものである。

【0 0 0 2】

【従来の技術】

図 1 5 は、従来例における送信装置と受信装置を示すブロック図である。図 1 5 において、4 9 は入力デジタルビデオ信号、5 0 は入力デジタルオーディオ信号、5 6 は M P E G - 2 ビデオ (I S O / I E C 1 3 8 1 8 - 2) に準拠したビデオ符号化手段、5 7 は M P E G - 2 オーディオ (I S O / I E C 1 3 8 1 8 - 3) に準拠したオーディオ符号化手段、6 4 はオーディオビットストリーム、7 6 はビデオビットストリーム、5 9 はプログラム仕様情報生成手段、5 0 0 はプログラム仕様情報、6 6 は M P E G - 2 システムズ (I S O / I E C - 1 3 8 1 8 - 1) に準拠した多重化手段、5 0 1 は多重化ビットストリーム、1 0 7 は多重化分離手段、1 1 0 はビデオビットストリーム、1 2 6 はオーディオビットストリーム、1 1 2 はビデオ復号手段、1 1 3 はオーディオ復号手段、1 1 1 はデジタルビデオ信号、1 1 4 はデジタルオーディオ信号、5 0 3 は受信装置である。

【0 0 0 3】

図 1 5 にて、従来の送信装置 5 0 2 では、入力デジタルビデオ信号 4 9 は、ビデオ符号化手段 5 6 によって M P E G - 2 ビデオに準拠して圧縮符号化されビデオビットストリーム 7 6 として出力される。入力デジタルオーディオ信号 5 0 は、オーディオ符号化手段 5 7 によって圧縮符号化されオーディオビットストリーム 6 4 として出力される。プログラム仕様情報生成手段 5 9 は、ビデオビットストリーム 7 6、オーディオビットストリーム 6 4 とプログラム番号との関係を示すプログラム仕様情報 5 0 0 を生成する。多重化手段 6 6 はビデオビットス

トリーム76、オーディオビットストリーム64、プログラム仕様情報500を多重化して多重化ビットストリーム501を生成する。

【0004】

従来の受信装置503では、多重化情報500は多重化分離手段107によってビデオビットストリーム110、オーディオビットストリーム126とに分離される。ビデオビットストリーム110はビデオ復号手段111によって伸長されデジタルビデオ信号112として出力される。オーディオビットストリーム126はオーディオ復号手段113によって伸長されデジタルオーディオ信号114として出力される。

【0005】

【発明が解決しようとする課題】

しかしながら、上記において、ビデオビットストリーム等の暗号化は行われておらず、不正な受信装置によって容易に盗むことが可能である。また、仮に暗号化を施しても暗号化手法自体を不正に解読されることに対する対処もなされていない。すなわち、送信装置が送信したデータの不正な受信を防ぐ手段がないという課題がある。

【0006】

本発明は、上記課題を考慮し、送信装置が送信したデータを受信装置が安全に受信する保護手段を提供することを目的とするものである。

【0007】

【課題を解決するための手段】

上述した課題を解決するために、第1の発明（請求項1に対応）は、データを暗号化して第1の暗号化データを生成する暗号化手段と、第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報手段と、第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第1の暗号化データに付随する権利情報を生成する権利情報生成手段と、第1の暗号化データと前記プログラム仕様情報と前記ツール

リストと前記制御グラフと前記権利情報とを多重化する多重化手段とを有する送信装置である。

【 0 0 0 8 】

また、第 2 の発明（請求項 2 に対応）は、データを暗号化して第 1 の暗号化データを生成する暗号化手段と、第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第 1 の暗号化データに付随する権利情報を生成する権利情報生成手段と、第 1 の暗号化データと第 1 の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、第 1 の暗号化データと前記プログラム仕様情報とを多重化する多重化手段とを有する送信装置である。

【 0 0 0 9 】

また、第 3 の発明（請求項 3 に対応）は、データを暗号化して第 1 の暗号化データを生成する暗号化手段と、第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第 1 の暗号化データと第 1 の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、前記データに付随する権利情報を生成する権利情報生成手段と、前記権利情報を出力する権利情報送信手段と、第 1 の暗号化データと前記プログラム仕様情報とを多重化して出力する多重化手段とを有する送信装置である。

【 0 0 1 0 】

また、第 4 の発明（請求項 4 に対応）は、前記権利情報と前記データとの対応付けを行う前記権利情報送信手段を有する第 3 の発明に記載の送信装置。

【 0 0 1 1 】

また、第 5 の発明（請求項 5 に対応）は、前記権利情報と前記データとの対応付けを行う前記プログラム仕様情報生成手段を有する第 3 の発明に記載の送信装

置である。

【 0 0 1 2 】

また、第 6 の発明（請求項 6 に対応）は、暗号を復号する復号ツールを多重化
する前記多重化手段を有する第 1 の発明乃至第 5 の発明いずれかに記載の送信装
置。

【 0 0 1 3 】

また、第 7 の発明（請求項 7 に対応）は、暗号を復号するための鍵情報を多重
化する前記多重化手段を有する第 1 の発明乃至第 6 の発明いずれかに記載の送信
装置。

【 0 0 1 4 】

また、第 8 の発明（請求項 8 に対応）は、第 1 の暗号化データを含む多重化信
号を少なくとも第 1 の暗号化データとプログラム仕様情報とに分離する多重化分
離手段と、前記多重化信号から第 1 の暗号化データを復号する復号ツールを示す
ツール ID を有するツールリストを分離するツールリスト分離手段と、前記多重
化信号から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離
する制御グラフ分離手段と、前記多重化信号から第 1 の暗号化データに付随する
権利情報を分離する権利情報手段と、前記ツールリストから取得したツール ID
に従ってツールを入手し、前記制御グラフに従って前記ツールを組み込む第 1 の
制御手段と、前記権利情報に従って第 1 の暗号化データを処理する第 1 の権利管
理手段とを有する受信装置である。

【 0 0 1 5 】

また、第 9 の発明（請求項 9 に対応）は、第 1 の暗号化データを含む多重化信
号を少なくとも第 1 の暗号化データとプログラム仕様情報とに分離する多重化分
離手段と、前記プログラム仕様情報から第 1 の暗号化データを復号する復号ツ
ールを示すツール ID を有するツールリストを分離するツールリスト分離手段と、
前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す
制御グラフを分離する制御グラフ分離手段と、前記プログラム仕様情報から第 1
の暗号化データに付随する権利情報を分離する権利情報手段と、前記ツールリス
トから取得したツール ID を有するツールを前記制御グラフに従って組み込む第

1 の制御手段と、前記権利情報に従って第 1 の暗号化データを処理する第 1 の権利管理手段とを有する受信装置である。

【 0 0 1 6 】

また、第 1 0 の発明（請求項 1 0 に対応）は、第 1 の暗号化データを含む多重化信号を少なくとも第 1 の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記プログラム仕様情報から第 1 の暗号化データを復号する復号ツールを示すツール ID を有するツールリストを分離するツールリスト分離手段と、前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記ツールリストから取得したツール ID を有するツールを前記制御グラフに従って組み込む第 1 の制御手段と、第 1 の暗号化データに付随する権利情報を受信する権利情報受信手段と、前記権利情報に従って第 1 の暗号化データを処理する第 1 の権利管理手段とを有する受信装置である。

【 0 0 1 7 】

また、第 1 1 の発明（請求項 1 1 に対応）は、受信した第 1 の暗号化データを一時的に記憶する一時記憶手段と、前記一時記憶手段に記憶された第 1 の暗号化データを読み取る読み取り手段を有する第 8 の発明乃至第 1 0 の発明いずれかに記載の受信装置である。

【 0 0 1 8 】

また、第 1 2 の発明（請求項 1 2 に対応）は、前記権利情報に記述された再生許諾が満了した後に第 1 の暗号化データを前記一時記憶手段から消去するファイル管理手段を有する第 1 1 の発明に記載の受信装置である。

【 0 0 1 9 】

また、第 1 3 の発明（請求項 1 3 に対応）は、第 1 の暗号化データの処理状態を示す状態情報を送信する前記権利管理手段を有する第 8 の発明乃至第 1 2 の発明いずれかに記載の受信装置である。

【 0 0 2 0 】

また、第 1 4 の発明（請求項 1 4 に対応）は、前記権利情報を第 1 の権利情報と第 2 の権利情報とに分割する権利管理手段と、前記多重化信号のうちの前記権

利情報を第 2 の権利情報に書き換えて修正多重化信号を出力する多重化修正手段と、第 2 の受信装置からの要求信号に応じて前記修正多重化信号を第 2 の受信装置に出力する第 8 の発明乃至第 1 2 の発明いずれかに記載の受信装置である。

【 0 0 2 1 】

また、第 1 5 の発明（請求項 1 5 に対応）は、前記権利情報を第 1 の権利情報と第 2 の権利情報とに分割する権利管理手段と、第 2 の受信装置からの要求信号に応じて第 2 の権利情報と前記多重化信号を第 2 の受信装置に出力する第 8 の発明乃至第 1 3 の発明いずれかに記載の受信装置である。

【 0 0 2 2 】

また、第 1 6 の発明（請求項 1 6 に対応）は、前記権利管理手段は第 2 の受信装置における第 1 の暗号化データの処理状態を示すデータを受信し自身と第 2 の受信装置の処理状態を示す状態情報を送信することを特徴とする第 8 の発明乃至第 1 5 の発明いずれかに記載の受信装置である。

【 0 0 2 3 】

また、第 1 7 の発明（請求項 1 7 に対応）は、第 1 の暗号化データを第 2 の暗号化データに変換する変換手段と、第 2 の暗号化データを第 2 の権利情報とともに再多重化する再多重化手段を有する第 8 の発明乃至第 1 6 の発明いずれかに記載の受信装置である。

【 0 0 2 4 】

また、第 1 8 の発明（請求項 1 8 に対応）は、第 1 の権利情報によって第 1 の暗号化データを処理する第 8 の発明乃至第 1 7 の発明いずれかに記載の受信装置である。

【 0 0 2 5 】

また、第 1 9 の発明（請求項 1 9 に対応）は、第 1 の暗号化データを第 2 の受信手段に転送後、前記第 1 の暗号化データを前記一次記憶手段から消去するファイル管理手段を有する第 1 4 の発明乃至第 1 8 の発明いずれかに記載の受信装置である。

【 0 0 2 6 】

また、第 2 0 の発明（請求項 2 0 に対応）は、前記多重化信号からビデオデー

タを抽出し復号するビデオ復号手段を有する第 8 の発明乃至第 1 9 の発明いずれかに記載の受信装置である。

【 0 0 2 7 】

また、第 2 1 の発明（請求項 2 1 に対応）は、前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する第 8 の発明乃至第 1 9 の発明いずれかに記載の受信装置である。

【 0 0 2 8 】

【発明の実施の形態】

以下、本発明の実施の形態について、図 1 ～図 1 4 を用いて説明する。

【 0 0 2 9 】

（第 1 の実施の形態）

図 1 は、本発明の第 1 の実施の形態における送信装置を示すブロック図である。図 1 において、4 9、5 0、5 6、5 7、5 9、6 4、7 6 は図 1 5 に示す従来例の構成と同様であり、5 1 は権利情報生成手段、5 2 はツールリスト生成手段、5 3 は制御グラフ生成手段、5 8 はストリーム情報生成手段、6 0 は A E S（Advanced Encryption Standard）に準拠した鍵長 1 2 8 ビットの暗号化を行う暗号化手段、6 1 はプログラム仕様情報生成手段、6 2 は M P E G - 2 システムズ（I S O / I E C - 1 3 8 1 8 - 1）に準拠した多重化手段、6 3 は暗号化ビデオビットストリーム、6 5 はプログラム仕様情報、6 6 は多重化ビットストリーム、6 7 は権利情報生成手段 5 1 によって生成される権利情報、6 8 はツールリスト生成手段 5 2 によって生成されるツールリスト、6 9 は制御グラフ生成手段 5 3 によって生成される制御グラフ、7 2 はストリーム情報、7 3 は第 1 の送信装置、7 4 は状態情報、7 5 は送信制御手段、8 1 は権利制御情報、8 2 はツール制御情報、8 3 はグラフ制御情報、1 1 5 は復号ツールである。

【 0 0 3 0 】

図 1 にて、入力デジタルビデオ信号 4 9 は、ビデオ符号化手段 5 6 によって M P E G - 2 準拠のビデオビットストリーム 7 6 に圧縮符号化され、第 1 の暗号化手段 6 0 によって暗号化され暗号化ビデオビットストリーム 6 3 として出力さ

れる。入力デジタルオーディオ信号 5 0 は、オーディオ符号化手段 5 7 によって圧縮符号化されオーディオビットストリーム 6 4 として出力される。

【 0 0 3 1 】

表 1 に状態情報 7 4 を示す。表 1 に示す各値は 8 ビットで表され、ビット 7 ～ビット 0 で表されるものとする。送信デバイス ID をもつ送信装置から受信デバイス ID をもつ受信装置との間で状態情報及び内容を交信する。状態情報は表 1 に示す各値をもつものとし、内容の項にその内容を記入する。

【 0 0 3 2 】

【表 1】

状態情報	
ツール要求	0X10000000
コンテンツ要求	0X01000000
コピー情報	0X00100000
再生回数	0X00010000
編集	0X00001000

【 0 0 3 3 】

権利情報生成手段 5 1 は、コンテンツ毎にコンテンツの利用条件を示す権利情報を作成してプログラム仕様情報生成手段 5 9 に供給する。表 2 の値は、状態情報が各々コピー情報、再生回数、編集である場合に対応して表 1 の内容のところに記入される。ここでプログラムとはコンテンツにプログラム仕様情報を付加した番組を示すことにする。

【 0 0 3 4 】

【表 2】

コピー情報	1 回	0X00000000
	禁止	0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【 0 0 3 5 】

本発明の第 1 の実施の形態では、A、B の 2 種類のプログラムを含むものとする。プログラム A は表 3 に示す値で送るものとする。すなわち、コピー 1 回、再生回数 1 回、編集禁止である。

【 0 0 3 6 】

【表 3】

コンテンツ		プログラムA
コピー	1 回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 0 3 7 】

プログラムBは表4に示す値で送るものとする。すなわち、コピー1回、再生回数3回、編集禁止である。

【 0 0 3 8 】

【表 4】

コンテンツ		プログラムB
コピー	1 回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【 0 0 3 9 】

送信装置73は、AES復号を実行するツールID（0X00A）を有する復号ツール115が存在することを認識しているものとする。ツールリスト生成手段52は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段59に供給する。ツールリスト生成手段52では、MPEG-2ビデオビットストリームを受信し再生するために復号ツール115が必要であることを示し上記ツールID（0X00A）を有するツールリストを生成する。

【 0 0 4 0 】

制御グラフ69の構成の一部を図2に示す。プログラムAは暗号化ビデオビットストリーム63とオーディオビットストリーム64を含み、暗号化ビデオビットストリーム63に対応するツールID、ツールの組み込み位置を示す制御ポイントを有している。プログラムBも同様である。

【 0 0 4 1 】

制御グラフ生成手段53は、AES復号を実行するツールID（0X00A）を有するツールの組み込み位置が受信装置のビデオ復号手段の直前であることを示す制御グラフ69を生成してプログラム仕様情報生成手段61に出力する。

【 0 0 4 2 】

プログラム仕様情報生成手段 6 1 は、暗号化ビデオビットストリーム 6 3 とオーディオビットストリーム 6 4 とプログラムのプログラム番号との関係を示す関係表とともに権利情報 6 7、ツールリスト 6 8、制御グラフ 6 9 を含むプログラム仕様情報 6 5 を生成する。

【 0 0 4 3 】

ストリーム情報生成手段 5 8 は、暗号化手段 6 0 で用いられている暗号を解く為の鍵情報などが入ったストリーム情報 7 2 を作成する。

【 0 0 4 4 】

多重化手段 6 2 は暗号化ビデオビットストリーム 6 3、オーディオビットストリーム 6 4、プログラム仕様情報 6 5、ストリーム情報 7 2、復号ツール 1 1 5 を M P E G - 2 システムズに準拠して多重化し、多重化ビットストリーム 6 6 を生成する。

【 0 0 4 5 】

また、送信制御手段 7 5 は状態情報 7 4 を他の機器から受け取ることによって、本発明の第 1 の実施の形態の送信装置が許諾した権利情報 6 7 が他の機器でどのように処理されたかを知ることができる。ここでは、表 4 に示すプログラム B の権利情報が表 5 に示す状態情報 7 4 として本発明の送信装置で受信されたとすると、1 回コピーされ、2 回再生されたことがわかる。

【 0 0 4 6 】

【表 5】

コンテンツ		プログラム B
コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【 0 0 4 7 】

以上のように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供するとともに、多重化情報のプログラ

ム仕様情報の一部として処理することができるという利便性を送信装置を提供することができる。

【 0 0 4 8 】

また、本発明の第 1 の実施の形態では、権利情報 6 7、ツールリスト 6 8、制御グラフ 6 9 をプログラム仕様情報生成手段 5 9 に加えているがプログラム仕様情報生成手段 5 9 を経ずに直接多重化情報生成手段 6 2 に加えてもよい。この場合には、権利情報 6 7、ツールリスト 6 8、制御グラフ 6 9 はプログラム仕様情報に含まれないのでより簡便な送信装置を提供することができる。

【 0 0 4 9 】

(第 2 の実施の形態)

図 3 は、本発明の第 2 の実施の形態における送信装置を示すブロック図である。図 3 において、4 9、5 0、5 6、5 7、6 4、7 6 は図 1 5 に示す従来例の構成と同様であり、5 1～5 3、5 8、6 0～6 3、6 5～6 9、7 2、7 4、7 5、8 1～8 3 は図 1 に示す本発明の第 1 の実施の形態と同様であり、8 4 は権利情報送信手段、8 5 は送信権利情報、8 6 は第 2 の送信装置である。

【 0 0 5 0 】

図 3 にて、入力ディジタルビデオ信号 4 9 は、ビデオ符号化手段 5 6 によって M P E G - 2 準拠のビデオビットストリーム 7 6 に圧縮符号化され、暗号化手段 6 0 によって暗号化され暗号化ビデオビットストリーム 6 3 として出力される。入力ディジタルオーディオ信号 5 0 は、オーディオ符号化手段 5 7 によって圧縮符号化されオーディオビットストリーム 6 4 として出力される。

【 0 0 5 1 】

状態情報 7 4 は表 1 と同様であり、権利情報生成手段 5 1 は、コンテンツ毎にコンテンツの利用条件を示す権利情報 6 7 を作成して権利情報送信手段 8 4 に供給する。表 6 に権利情報 6 7 を示す。

【 0 0 5 2 】

【表 6】

コピー	1 回	0X00000000
	禁止	0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【 0 0 5 3 】

本発明の第 2 の実施の形態では、プログラム A、プログラム B の 2 種類のコンテンツを含むものとする。プログラム A は表 7 に示す値で送るものとする。すなわち、コピー 1 回、再生回数 1 回、編集禁止である。表 7 で権利情報はプログラム A との対応付けが行われている。

【 0 0 5 4 】

【表 7】

コンテンツ		プログラム A
コピー	1 回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 0 5 5 】

プログラム B は表 8 に示す値で送るものとする。すなわち、コピー 1 回、再生回数 3 回、編集禁止である。表 8 で権利情報はプログラム B との対応付けが行われている。

【 0 0 5 6 】

【表 8】

コンテンツ		プログラム B
コピー	1 回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【 0 0 5 7 】

送信装置 8 6 は、A E S 復号を実行するツール I D (0 X 0 0 A) を有する復号ツール 1 1 5 があることを認識しているものとする。ツールリスト生成手段 5 2 は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段 6 1 に供給する。すなわち、M P E G - 2 ビデオビットストリームを受

信し再生するために復号ツール 115 が必要であることを示し上記ツール ID (0X00A) を有するツールリスト 68 を生成する。

【0058】

制御グラフの構成は図 2 と同様である。プログラム A は第 1 の暗号化ビットストリーム 63 とオーディオビットストリーム 64 を含み、第 1 の暗号化ビットストリーム 63 に対応するツール ID、ツールが組み込まれる組み込み位置を示す制御ポイントを有している。プログラム B も同様である。

【0059】

制御グラフ生成手段 53 は、上記 AES 復号を実行するツール ID (0X00A) を有するツールの組み込み位置が受信装置のビデオ復号手段の手前であることを示す制御グラフ 69 を生成してプログラム仕様情報生成手段 61 に出力する。

【0060】

プログラム仕様情報生成手段 61 は、暗号化ビデオビットストリーム 63 とオーディオビットストリーム 64 とプログラムのプログラム番号との関係を示す関係表とともにツールリスト 68、制御グラフ 69 と復号ツール 115 を含むプログラム仕様情報 65 を生成する。

【0061】

ストリーム情報生成手段 58 は、暗号化手段 60 で用いられている暗号を解く為の鍵情報などが入ったストリーム情報 72 を作成する。

【0062】

多重化手段 62 は暗号化ビデオビットストリーム 63、オーディオビットストリーム 64、プログラム仕様情報 65、ストリーム情報 72 を上記 MPEG-2 システムズに準拠して多重化し、多重化ビットストリーム 66 を生成する。

【0063】

権利情報送信手段 84 は、権利情報 67 とプログラムとの対応付けを行う。ここでは、プログラム仕様情報生成手段との通信によって暗号化ビデオビットストリーム 63 とオーディオビットストリーム 64 とプログラムのプログラム番号との関係を示す関係表が得られるのでプログラムとの対応付けを行うことができ、

その後、ファイル化して送信権利情報 8 5 として送信する。権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利点がある。

【 0 0 6 4 】

また、送信制御手段 7 5 は状態情報 7 4 を他の機器から受け取ることによって、本発明の第 1 の実施の形態の送信装置が許諾した権利情報 6 7 が他の機器でどのように処理されたかを知ることができる。ここでは、表 8 に示す権利情報が表 9 に示す権利情報として本発明の送信装置で受信されたとすると、1 回コピーされ、2 回再生されたことがわかる。

【 0 0 6 5 】

【表 9】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【 0 0 6 6 】

以上のように、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供するとともに、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を送信装置を提供することができる。

【 0 0 6 7 】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【 0 0 6 8 】

(第 3 の実施の形態)

図 4 は、本発明の第 3 の実施の形態における受信装置を示すブロック図である。図 4 において、111～114 は図 15 に示す従来例の構成と同様であり、100 は第 1 の受信装置、101 は入力される M P E G - 2 システムズ準拠の第 1 の多重化ビットストリーム、102 はハードディスク記憶手段、103 はハードディスク記憶手段 102 から読み出された読み出し多重化ビットストリーム、108 は組み込み手段、110 はビデオビットストリーム、115 は A E S 暗号を復号する復号ツール、120 は第 1 の制御手段、121 は第 1 の権利管理手段、123 はファイル管理情報、124 はファイル管理手段、125 はハードディスク 102 に対する指令、90 はストリーム情報及び復号ツール 115 を含む読み出し情報、91 はプログラム仕様情報分離手段、92 はプログラム仕様情報、93 は制御グラフ分離手段、94 は制御グラフ情報、95 はツールリスト分離手段、96 はツールリスト、97 は権利情報分離手段、98 は権利情報、132 は第 1 の返信情報、137 は第 1 の要求情報である。また、第 1 の受信装置 100 は第 1 の送信装置 73 に接続されているものとする。

【0069】

図 4 にて、入力される M P E G - 2 システムズ準拠の第 1 の多重化ビットストリーム 101 はハードディスク 102 に一時的に記憶された後に読み出され読み出し多重化ビットストリーム 103 として多重化分離手段 104 に加えられる。多重化分離手段 104 は読み出し多重化ビットストリーム 103 を第 1 の暗号化ビデオビットストリーム 105 とオーディオビットストリーム 106 とプログラム仕様情報 92 とストリーム情報 90 とに分離する。

【0070】

ここで、プログラム仕様情報 92 は、第 1 の暗号化ビデオビットストリーム 105、オーディオビットストリーム 64 とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報 98 と A E S 復号を実行するツール I D (0 X 0 0 A) を有するツールリスト 96 と上記復号ツールの組み込み位置が受信装置 100 の多重化分離手段 104 とビデオ復号手段 112 との間であることを示す制御グラフ 94 を含むものとする。また、読み出し情報

9 0 には、第 1 の暗号化ビデオビットストリーム 1 0 5 の暗号を解く為の鍵情報などが入っているものとする。

【 0 0 7 1 】

読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 1 の制御手段 1 2 0 に加えられる。プログラム仕様情報 9 2 はプログラム仕様情報分離手段 9 1 に加えられる。制御グラフ分離手段 9 3 はプログラム仕様情報分離手段 9 1 から制御グラフ 9 4 を抽出して第 1 の制御手段 1 2 0 に供給する。ツールリスト分離手段 9 5 はプログラム仕様情報分離手段 9 1 からツールリスト 9 6 を抽出して第 1 の制御手段 1 2 0 に供給する。権利情報分離手段 9 7 はプログラム仕様情報分離手段 9 1 から権利情報 9 8 を抽出して第 1 の権利管理手段 1 2 1 に供給する。

【 0 0 7 2 】

第 1 の制御手段 1 2 0 は表 1 0 に示す第 1 の要求情報 1 3 7 を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【 0 0 7 3 】

【表 1 0】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【 0 0 7 4 】

第 1 の制御手段 1 2 0 は、ツールリスト 9 6 から復号に必要なツールが復号ツール 1 1 5であることを求め、制御グラフ 9 4 から復号ツール 1 1 5を適用する制御ポイントすなわち組み込み位置が 1 0 8であることを求めるとともに読み出し情報 9 0 からスクランブルを解くための鍵情報を抽出する。

【 0 0 7 5 】

第 1 の制御手段 1 2 0 は、復号ツール 1 1 5の組み込み位置が受信装置 1 0 0 の多重化分離手段 1 0 4 とビデオ復号手段 1 1 2 との間であることを示す制御グラフ 9 4 に従って、組み込み手段 1 0 8 に復号ツール 1 1 5とストリーム情報 1 1 8 から抽出された上記鍵情報が組み込む指示を出し、組み込み手段 1 0 8 は復号ツール 1 1 5と上記鍵情報を組み込む。第 1 の暗号化ビデオビットストリーム 1 0 5 は組み込み手段 1 0 8 によって暗号を解読されてビデオビットストリーム

1 1 0として出力される。

【0 0 7 6】

ビデオビットストリーム 1 1 0はビデオ復号手段 1 1 1によって伸長されデジタルビデオ信号 1 1 2として出力される。オーディオビットストリーム 1 0 6はオーディオ復号手段 1 1 3によって伸長されデジタルオーディオ信号 1 1 4として出力される。

【0 0 7 7】

第 1 の権利管理手段 1 2 1は権利情報 9 8を取得し、ファイル管理情報 1 2 3をファイル管理手段 1 2 4に出力する。ファイル管理手段 1 2 4は、プログラム Aの場合、表 4に与えられた再生回数は 1 回であるため、1 回再生するとファイル管理手段 1 2 4は、指令 1 2 5をハードディスク 1 0 2に出してハードディスク 1 0 2上に記憶されたプログラム Aを消去する。

【0 0 7 8】

また、第 1 の権利管理手段 1 2 1は第 2 の返信情報 1 3 2として表 1 1に示す情報を返信する。ここでは第 1 の受信装置 1 0 0で 1 回再生されている。

【0 0 7 9】

【表 1 1】

コピー	許可	0X00000000
第 1 の受信装置での再生回数		0X00000001

【0 0 8 0】

(第 4 の実施の形態)

図 5は、本発明の第 4 の実施の形態における受信装置を示すブロック図である。本発明の第 4 の実施の形態は受信装置がネットワークを通じて接続されている別の受信装置にツールをダウンロード、デジタルデータを転送、サーバに消費情報を転送することができる。図 5において、1 1 1～1 1 4は図 1 5に示す従来例の構成と同様であり、9 0～9 8、1 0 1～1 0 6、1 0 8、1 1 0、1 1 5、1 2 3～1 2 5、1 3 2は本発明の第 3 の実施の形態と同様であり、1 3 0は第 2 の受信装置、1 3 3は第 2 の権利情報、1 3 6は第 2 の返信情報、1 3 8は第 2 の権利管理手段、1 3 9は第 2 の制御手段、1 4 0は第 2 の要求情報、1

4 1 は第 1 の制御情報、1 4 2 は多重化修正手段、1 4 3 は M P E G - 2 システムズ準拠の第 2 の多重化ビットストリーム、1 4 4 は第 1 0 の受信装置である。図 6 は、第 2 の権利管理手段 1 3 8 の処理の概略を示す図である。図 7 は、第 1 の多重化ビットストリーム 1 0 3 と第 2 の多重化ビットストリーム 1 4 3 の概略の構成を示す図であり、1 4 6 は暗号化ビデオビットストリーム 6 3 とオーディオビットストリーム 6 4 とプログラム A のプログラム番号との関係を示す関係表である。また、図 5 において、第 2 の受信装置 1 3 0 は送信装置 7 3 に接続されているものとし、第 2 の受信装置 1 3 0 に接続されている第 1 0 の受信装置 1 4 4 は図 4 に示す第 1 の受信装置と等価な機能を有するものとする。

【 0 0 8 1 】

図 5 にて、読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 2 の制御手段 1 3 9 に加えられる。第 2 の制御手段 1 3 9 は、第 2 の権利管理手段 1 3 8 に権利許諾の情報を出すとともに多重化修正手段 1 4 2 に多重化ビットストリーム修正を含む第 1 の制御情報 1 4 1 を送る。

【 0 0 8 2 】

第 2 の制御手段 1 3 9 は第 1 0 の受信装置 1 4 4 から表 1 2 に示す第 2 の要求情報 1 4 0 を受け取る。表 1 2 は第 1 0 の受信装置 1 4 4 が第 2 の受信装置 1 3 0 に対してツールとコンテンツを要求していることを示している。

【 0 0 8 3 】

【表 1 2】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【 0 0 8 4 】

図 6 は第 2 の権利管理手段 1 3 8 の動作の一部を示している。ステップ 1 において、第 2 の制御手段 1 3 9 を経由して第 2 の要求情報 1 4 0 を受信する、ステップ 2 で権利情報 9 8 を受信し、ステップ 3 で権利情報 9 8 を第 2 の受信装置 1 3 0 で使用する第 1 の権利情報と第 1 0 の受信装置 1 4 4 で使用する第 2 の権利情報 1 3 3 に分割する。ステップ 4 で第 1 の権利情報を出力し、ステップ 5 で第 1 の権利情報に基づいてファイル管理情報 1 2 3 をファイル管理手段 1 2 4 に出

力し、ステップ6で第2の権利情報133を出力する。

【0085】

第2の受信装置130で表4に示す権利情報を有するプログラムBを1回再生するとともに第1の受信装置に転送するものとする、第1の権利情報を表13、第2の権利情報を表14のように表わすことができる。第10の受信装置144に転送する第2の権利情報を示す表14では第2の受信装置130で1回再生するので再生回数を1回減じている。

【0086】

【表13】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【0087】

【表14】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【0088】

第2の権利管理手段138は表14に示す第2の権利情報133を多重化修正手段142に送る。多重化修正手段142は第1の多重化ビットストリーム103に第2の権利情報133をもとに修正を加える。すなわち、第1の多重化ビットストリーム103の権利情報122を第2の権利情報133の内容に変更して第2の多重化ビットストリーム143を出力する。

【0089】

図7は第1の多重化ビットストリームと第2の多重化ビットストリームの構成を示している。権利情報98は第2の権利管理手段によって第2の権利情報133として多重化修正手段142に加えられ、第2の多重化ビットストリーム143では第2の権利情報が含まれる。

【0090】

第2の制御手段139は、復号ツール115の組み込み位置が第2の受信装置130の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94に従って、組み込み手段108に復号ツール115とストリーム情報118から抽出された上記鍵情報を組み込む指示を出し、組み込み手段108は復号ツール115と上記鍵情報を組み込む。第1の暗号化ビデオビットストリーム105は組み込み手段108によって暗号を解読されてビデオビットストリーム110として出力され、ビデオ復号手段112によって復号されてデジタルビデオ信号として出力される。

【0091】

その他の動作は本発明の第3の実施の形態と同様である。これによって、第2の受信装置130は、受信した権利情報、ビットストリーム、ツール情報等をネットワーク上で接続された第10の受信装置144に送ることが可能となる。

【0092】

また、第2の権利管理手段138は、第10の受信装置144から送られる第2の返信情報136をもとにして第1の返信情報132を出力する。この場合、第2の受信装置130及び第10の受信装置144での再生回数は1回であるとする、表15のように構成される第1の返信情報を出力する。

【0093】

【表15】

第2の受信装置での再生回数	0X00000001
第1の受信装置での再生回数	0X00000001

【0094】

これによって送信装置は、第2の受信装置130及び第2の受信装置130に接続された第10の受信装置144での消費情報を得ることができる。

【0095】

(第5の実施の形態)

図8は、本発明の第5の実施の形態における受信装置を示すブロック図である。本発明の第5の実施の形態は受信装置が受信した権利情報をダウンロード、デジタルデータをネットワークに接続されている別の受信装置に転送するととも

にサーバに消費情報を転送することができる。図 8 において、111～114 は図 15 に示す従来例の構成と同様であり、90～98、101～106、108、110、115、123～125、132、137 は図 4 に示す本発明の第 3 の実施の形態と同様であり、136、140 は図 5 に示す本発明の第 4 の実施の形態と同様であり、150 は第 3 の受信装置、153 は第 3 の権利情報、154 は第 4 の受信装置、160 は第 3 の制御手段、161 は第 3 の権利管理手段である。

【0096】

図 8 にて、第 3 の制御手段 160 は第 4 の受信装置 154 から表 16 に示す第 2 の要求情報 140 を受け取るものとする。表 16 は第 4 の受信装置 154 が第 3 の受信装置 150 に対してツールとコンテンツを要求していることを示している。第 3 の制御手段 160 は第 3 の権利管理手段 161 に権利許諾の情報を出す。

【0097】

【表 16】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0098】

読み出し情報 90 は多重化分離手段 104 で分離されて第 3 の制御手段 160 に加えられる。第 3 の権利管理手段 161 は、権利情報 98 を第 3 の受信装置 150 で使用する第 1 の権利情報と第 4 の受信装置 154 で使用する第 3 の権利情報 153 とに分割し、第 3 の権利情報 153 を第 4 の受信装置 154 に送る。

【0099】

ここでは第 3 の受信装置 150 で 1 回再生し、第 4 の受信装置 154 で 1 回再生するものとする。第 1 の権利情報及び第 3 の権利情報 153 は各々表 17、表 18 となる。表 18 では第 3 の受信装置 150 で 1 回再生しているので再生回数を 1 回減じている。

【0100】

【表 1 7】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 1 0 1】

【表 1 8】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【 0 1 0 2】

その他の動作は本発明の第 3 の実施の形態と同様である。これによって、第 3 の受信装置 1 5 0 は、受信した権利情報、ビットストリーム、ツール情報等を第 4 の受信装置 1 5 4 に送ることが可能となる。

【 0 1 0 3】

(第 6 の実施の形態)

図 9 は、本発明の第 6 の実施の形態における受信装置を示すブロック図である。本発明の第 6 の実施の形態は第 3 の受信装置にホームネットワークを経由して接続された第 4 の受信装置に関するものである。図 9 において、1 1 1 ~ 1 1 4 は図 1 5 に示す従来例の構成と同様であり、9 0 ~ 9 8、1 0 1 ~ 1 0 6、1 0 8、1 1 0、1 1 5、1 2 3 ~ 1 2 5、1 3 7 は図 4 に示す本発明の第 3 の実施の形態と同様であり、1 3 6 は図 5 に示す本発明の第 4 の実施の形態と同様であり、1 5 4 は第 4 の受信装置、2 3 1 は第 4 の制御手段、2 3 2 は第 4 の権利管理手段である。

【 0 1 0 4】

図 9 にて、読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 4 の制御手段 2 3 1 に加えられる。第 4 の権利管理手段 2 3 2 は権利情報 9 8 をもとにして、第 4 の受信装置 1 5 4 での消費状況とをもとに第 2 の返信情報 1 3 6 を生成する。第 2 の返信情報 1 3 6 は、デジタルビデオ情報 1 1 2 及びデジタルオーディオ情報 1 1 4 を第 4 の受信装置で再生したことを示す消費情報として再生

回数を 1 回減じる。その結果、表 1 8 のように与えられるプログラム B の権利情報は表 1 9 のように書き換えられる。

【0 1 0 5】

【表 1 9】

コンテンツ	許可	プログラム B
コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【0 1 0 6】

表 1 9 のように書き換えられた第 2 の返信情報 1 3 6 は第 4 の権利管理手段 2 3 2 から送出される。その他の動作は図 4 に示す本発明の第 3 の実施の形態と同様である。

【0 1 0 7】

(第 7 の実施の形態)

図 1 0 は、本発明の第 7 の実施の形態における受信装置を示すブロック図である。本発明の第 7 の実施の形態は受信装置に受信した権利情報をダウンロード、デジタルデータを別の受信装置にデータを変換して転送するとともにサーバに消費情報を転送することができる。図 1 0 において、1 1 1 ~ 1 1 4 は図 1 5 に示す従来例の構成と同様であり、9 0 ~ 9 8、1 0 1 ~ 1 0 6、1 1 0、1 1 5、1 2 3 ~ 1 2 5、1 3 2 は、図 4 に示す本発明の第 3 の実施の形態と同様であり、1 4 1 は図 5 に示す本発明の第 4 の実施の形態と同様であり、1 4 4 は第 4 の権利情報、2 5 0 は第 5 の受信装置、2 5 1 は第 5 の権利管理手段、2 5 2 は第 5 の制御手段、2 5 3 は変換手段、2 5 4 は第 2 の暗号化ビデオビットストリーム、2 5 5 は再多重化手段、2 5 6 は M P E G - 2 システムズ準拠の第 3 の多重化ビットストリーム、2 5 7 は第 6 の受信装置、2 5 8 は第 3 の要求情報である。

【0 1 0 8】

図 1 0 にて、読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 5 の制御手段 2 5 2 に加えられる。第 5 の権利管理手段 2 5 1 は、権利情報 9 8 を第 5 の受信装置 2 5 0 で使用する第 1 の権利情報と第 6 の受信装置 2 5 7 で使用する

第 4 の権利情報 1 4 4 に分割し、第 4 の権利情報 1 4 4 を再多重化手段 2 5 5 に送る。

【 0 1 0 9 】

第 5 の制御手段 2 5 2 は第 6 の受信装置 2 5 7 から表 2 0 に示す第 3 の要求情報 2 5 8 を受け取るものとする。表 2 0 は第 6 の受信装置 2 5 7 が第 5 の受信装置 2 5 0 に対してツールとコンテンツを要求していることを示している。第 5 の制御手段 2 5 2 は第 5 の権利管理手段 2 5 1 に権利許諾の情報を出すとともに再多重化手段 2 5 5 に再多重化の指示を含む第 1 の制御情報 1 4 1 を送る。

【 0 1 1 0 】

【表 2 0】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【 0 1 1 1 】

ここで、第 5 の受信装置 2 5 0 で 1 回再生し、第 6 の受信装置 2 5 7 で 1 回再生するものとする、第 1 の権利情報及び第 4 の権利情報 1 4 4 は各々表 2 1、表 2 2 となる。表 2 2 では第 5 の受信装置 2 5 0 で 1 回再生しているので再生回数を 1 回減じている。

【 0 1 1 2 】

【表 2 1】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 1 1 3 】

【表 2 2】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【 0 1 1 4 】

変換手段 2 5 3 はデジタルビデオデータ 1 1 1 を M P E G - 4 ビデオ (I S

○／I E C 1 4 4 9 6) に圧縮変換し更に暗号化して第 2 の暗号化ビデオビットストリーム 2 5 4 を出力する。

【 0 1 1 5 】

復号ツール 1 1 5 は再多重化手段 2 5 5 に送られる。再多重化手段 2 5 5 は第 2 の暗号化ビデオビットストリーム 2 5 4 とオーディオビットストリーム 1 2 6 と第 1 の制御情報 1 4 1 と第 4 の権利情報 1 4 4 と復号ツール 1 1 5 とを M P E G - 2 システムズに準拠して再多重し、再多重化信号 2 5 6 を出力する。本発明の第 7 の実施の形態ではデジタルオーディオビットストリーム 1 0 6 を用いているがデジタルオーディオ信号 1 1 4 を再度圧縮して用いてもよい。

【 0 1 1 6 】

その他の動作は図 4 に示す本発明の第 3 の実施の形態と同様である。これによって、第 5 の受信装置 2 5 0 は、受信した権利情報、ビットストリーム、ツール情報等を第 6 の受信装置 2 5 7 に送ることが可能となる。

【 0 1 1 7 】

(第 8 の実施の形態)

図 1 1 は、本発明の第 8 の実施の形態における受信装置を示すブロック図である。図 1 1 において、1 1 1 ～ 1 1 4 は図 1 5 に示す従来例の構成と同様であり、9 0 ～ 9 6、9 8、1 0 1 ～ 1 0 6、1 1 0、1 1 5、1 2 0、1 2 1、1 2 3 ～ 1 2 5、1 3 2 は、図 4 に示す本発明の第 3 の実施の形態と同様であり、3 0 0 は受信権利情報、3 0 1 は権利情報受信手段、3 0 2 は第 7 の受信装置である。また、第 7 の受信装置は本発明の第 2 の実施の形態の図 3 に示す送信装置 8 6 に接続されているものとする。本発明の第 8 の実施の形態は本発明の第 3 の実施の形態と類似であるが、権利情報 9 8 をプログラム仕様情報 9 2 でなく受信権利情報 3 0 0 から取得する点異なる。

【 0 1 1 8 】

図 1 1 にて、入力される M P E G - 2 システムズ準拠の第 1 の多重化ビットストリーム 1 0 1 はハードディスク 1 0 2 に一時的に記憶された後に読み出され読み出し多重化ビットストリーム 1 0 3 として多重化分離手段 1 0 4 に加えられる。多重化分離手段 1 0 4 は読み出し多重化ビットストリーム 1 0 3 を第 1 の暗号

化ビデオビットストリーム 1 0 5 とオーディオビットストリーム 1 0 6 とプログラム仕様情報 9 2 とストリーム情報 9 0 とに分離する。

【 0 1 1 9 】

ここで、プログラム仕様情報 9 2 は、第 1 の暗号化ビデオビットストリーム 1 0 5、オーディオビットストリーム 6 4 とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報 9 8 と A E S 復号を実行するツール I D (0 X 0 0 A) を有するツールリスト 9 6 と上記復号ツールの組み込み位置が受信装置 1 0 0 の多重化分離手段 1 0 4 とビデオ復号手段 1 1 2 との間であることを示す制御グラフ 9 4 を含むものとする。また、読み出し情報 9 0 には、第 1 の暗号化ビデオビットストリーム 1 0 5 の暗号を解く為の鍵情報などが入っているものとする。

【 0 1 2 0 】

読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 1 の制御手段 1 2 0 に加えられる。プログラム仕様情報 9 2 はプログラム仕様情報分離手段 9 1 に加えられる。制御グラフ分離手段 9 3 はプログラム仕様情報分離手段 9 1 から制御グラフ 9 4 を抽出して第 1 の制御手段 1 2 0 に供給する。ツールリスト分離手段 9 5 はプログラム仕様情報分離手段 9 1 からツールリスト 9 6 を抽出して第 1 の制御手段 1 2 0 に供給する。権利情報受信手段 3 0 1 は受信権利情報 3 0 0 を受信して権利情報 9 8 を抽出して出力し第 1 の権利管理手段 1 2 1 に供給する。

【 0 1 2 1 】

第 1 の制御手段 1 2 0 は表 2 3 に示す第 1 の要求情報 1 3 7 を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【 0 1 2 2 】

【表 2 3】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【 0 1 2 3 】

第 1 の制御手段 1 2 0 は、ツールリスト 9 6 から復号に必要なツールが復号ツール 1 1 5 であることを求め、制御グラフ 9 4 から復号ツール 1 1 5 を適用する

制御ポイントすなわち組み込み位置が 1 0 8 であることを求めるとともに読み出し情報 9 0 から暗号を解くための鍵情報を抽出する。

【 0 1 2 4 】

第 1 の制御手段 1 2 0 は、復号ツール 1 1 5 の組み込み位置が第 7 の受信装置 3 0 2 の多重化分離手段 1 0 4 とビデオ復号手段 1 1 2 との間であることを示す制御グラフ 9 4 に従って、組み込み手段 1 0 8 に復号ツール 1 1 5 とストリーム情報 1 1 8 から抽出された上記鍵情報を組み込む指示を出し、組み込み手段 1 0 8 は復号ツール 1 1 5 と上記鍵情報を組み込む。第 1 の暗号化ビデオビットストリーム 1 0 5 は組み込み手段 1 0 8 によって暗号を解読されてビットストリーム 1 1 0 として出力される。

【 0 1 2 5 】

ビデオビットストリーム 1 1 0 はビデオ復号手段 1 1 2 によって伸長されデジタルビデオ信号 1 1 1 として出力される。オーディオビットストリーム 1 0 6 はオーディオ復号手段 1 1 3 によって伸長されデジタルオーディオ信号 1 1 4 として出力される。

【 0 1 2 6 】

第 1 の権利管理手段 1 2 1 は権利情報 9 8 を取得し、ファイル管理情報 1 2 3 をファイル管理手段 1 2 4 に出力する。ファイル管理手段 1 2 4 は、プログラム A の場合、表 4 に与えられた再生回数は 1 回であるため、1 回再生するとファイル管理手段 1 2 4 は、指令 1 2 5 をハードディスク 1 0 2 に出してハードディスク 1 0 2 上に記憶されたプログラム A を消去する。

【 0 1 2 7 】

また、第 1 の権利管理手段 1 2 1 は第 1 の返信情報 1 3 2 として表 2 4 に示す情報を返信する。

【 0 1 2 8 】

【表 2 4】

第 7 の受信装置での再生回数	0X00000001
-----------------	------------

【 0 1 2 9 】

(第 9 の実施の形態)

図 1 2 は、本発明の第 9 の実施の形態における受信装置を示すブロック図である。本発明の第 9 の実施の形態はネットワークに接続されている受信装置に受信した権利情報をダウンロード、デジタルデータを転送するとともにサーバに消費情報を転送することができる。図 1 2 において、1 1 1 ~ 1 1 4 は図 1 5 に示す従来例の構成と同様であり、9 0 ~ 9 6、9 8、1 0 1 ~ 1 0 6、1 1 0、1 1 5、1 2 3 ~ 1 2 5、1 3 2 は本発明の第 3 の実施の形態と同様であり、1 3 3、1 3 6、1 3 8 ~ 1 4 0、1 4 1 ~ 1 4 3 は図 5 に示す本発明の第 4 の実施の形態と同様であり、3 0 0、3 0 1 は図 1 1 に示す本発明の第 8 の実施の形態と同様であり、3 1 0 は第 8 の受信装置、1 4 5 は第 1 1 の受信装置である。尚、第 8 の受信装置 3 1 0 は図 3 に示す本発明の第 2 の送信装置に接続されているものとし、第 1 1 の受信装置は、図 4 に示す第 1 の受信装置と同等の機能を有するものとする。

【 0 1 3 0 】

図 1 2 にて、制御グラフ分離手段 9 3 はプログラム仕様情報分離手段 9 1 から制御グラフ 9 4 を抽出して第 2 の制御手段 1 3 9 に供給する。ツールリスト分離手段 9 5 はプログラム仕様情報分離手段 9 1 からツールリスト 9 6 を抽出して第 2 の制御手段 1 3 9 に供給する。権利情報受信手段 3 0 1 は受信権利情報 3 0 0 を受信して権利情報 9 8 を抽出して出力し第 2 の権利管理手段 1 3 8 に供給する。

【 0 1 3 1 】

第 2 の制御手段 1 3 9 は第 1 1 の受信装置 1 4 5 から表 2 5 に示す第 2 の要求情報 1 4 0 を受け取るものとする。表 2 5 は第 1 1 の受信装置 1 4 5 が第 2 の受信装置 1 3 0 に対してツールとコンテンツを要求していることを示している。

【 0 1 3 2 】

【表 2 5】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【 0 1 3 3 】

また、読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 2 の制御手段 1 3 9 に加えられる。第 2 の権利管理手段 1 3 8 は、権利情報 9 8 を第 2 の受信装置 1 3 0 で使用する第 1 の権利情報と第 1 1 の受信装置 1 4 5 で使用する第 2 の権利情報 1 3 3 に分割するとともに、第 1 の権利情報に基づいてファイル管理情報 1 2 3 をファイル管理手段 1 2 4 に出力する。第 2 の権利管理手段 1 3 8 に権利許諾の指示を出すとともに多重化修正手段 1 4 2 に第 1 の多重化ビットストリーム 1 0 3 の修正を含む第 1 の制御情報 1 4 1 を送る。

【 0 1 3 4 】

第 8 の受信装置 3 1 0 で表 4 に示す権利情報を有するプログラム B を 1 回再生するとともに第 1 1 の受信装置 1 4 5 に転送するものとする、第 1 の権利情報を表 2 6、第 2 の権利情報 1 3 3 を表 2 7 のように表わすことができる。第 1 1 の受信装置 1 4 5 に転送する第 2 の権利情報を示す表 2 7 では第 2 の受信装置 1 3 0 で 1 回再生するので再生回数を 1 回減じている。

【 0 1 3 5 】

【表 2 6】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 1 3 6 】

【表 2 7】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【 0 1 3 7 】

第 2 の権利管理手段 1 3 8 は表 1 4 に示す第 2 の権利情報 1 3 3 を多重化修正手段 1 4 2 に送る。多重化修正手段 1 4 2 は第 1 の多重化ビットストリーム 1 0 3 に第 2 の権利情報 1 3 3 をもとに修正を加える。すなわち、第 1 の多重化ビットストリーム 1 0 3 の権利情報 1 2 2 を第 2 の権利情報 1 3 3 の内容に変更して第 2 の多重化ビットストリーム 1 4 3 を出力する。

【 0 1 3 8 】

その他の動作は本発明の第 4 の実施の形態と同様である。これによって、第 8 の受信装置 1 3 0 は、受信した権利情報、ビットストリーム、ツール情報等をネットワーク上で接続された第 1 1 の受信装置 1 4 5 に送ることが可能となる。

【 0 1 3 9 】

また、第 2 の権利管理手段 1 3 8 は、第 1 1 の受信装置 1 4 5 から送られる第 2 の返信情報をもとにして第 1 の返信情報 1 3 2 を出力する。この場合、第 8 の受信装置 3 1 0 及び第 1 1 の受信装置 1 4 5 での再生回数は 1 回であるとする、表 2 8 のように構成される第 1 の返信情報を出力する。

【 0 1 4 0 】

【表 2 8】

第 2 の受信装置での再生回数	0X00000001
第 1 0 の受信装置での再生回数	0X00000001

【 0 1 4 1 】

これによって送信装置は、第 8 の受信装置 3 1 0 及び第 8 の受信装置 3 1 0 に接続された第 1 1 の受信装置 1 4 5 での消費情報を得ることができる。

【 0 1 4 2 】

(第 1 0 の実施の形態)

図 1 3 は、本発明の第 1 0 の実施の形態における受信装置を示すブロック図である。本発明の第 1 0 の実施の形態は受信装置にホームネットワークを経由して接続された別の受信装置に関するものである。図 1 3 において、1 1 1 ~ 1 1 4 は図 1 5 に示す従来例の構成と同様であり、9 0 ~ 9 6、9 8、1 0 1 ~ 1 0 6、1 1 0、1 1 5、1 2 3 ~ 1 2 5、1 3 2 は図 4 に示す本発明の第 3 の実施の形態と同様であり、1 3 6、1 4 0 は図 5 に示す本発明の第 4 の実施の形態と同様であり、1 5 3、1 5 4、1 6 0、1 6 1 は図 8 に示す本発明の第 5 の実施の形態と同様であり、3 0 0、3 0 1 は図 1 1 に示す本発明の第 8 の実施の形態と同様であり、3 2 0 は第 9 の受信装置である。

【 0 1 4 3 】

図 1 3 にて、制御グラフ分離手段 9 3 はプログラム仕様情報分離手段 9 1 から

制御グラフ 94 を抽出して第 3 の制御手段 160 に供給する。ツールリスト分離手段 95 はプログラム仕様情報分離手段 91 からツールリスト 96 を抽出して第 3 の制御手段 160 に供給する。権利情報受信手段 301 は受信権利情報 300 を受信して権利情報 98 を抽出して出力し第 3 の権利管理手段 161 に供給する。

【0144】

また、読み出し情報 90 は第 3 の制御手段 160 に加えられる。第 3 の権利管理手段 161 は、権利情報 98 を第 9 の受信装置 320 で使用する第 1 の権利情報と第 4 の受信装置 154 で使用する第 3 の権利情報 153 とに分割し、第 3 の権利情報 153 を第 4 の受信装置 154 に送る。

【0145】

第 3 の制御手段 160 は第 4 の受信装置 154 から表 28 に示す第 2 の要求情報 140 を受け取るものとする。表 29 は第 4 の受信装置 154 が第 9 の受信装置 320 に対してツールとコンテンツを要求していることを示している。第 3 の制御手段 160 は第 3 の権利管理手段 161 に権利許諾の情報を出す。

【0146】

【表 29】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0147】

ここでは第 9 の受信装置 320 で 1 回再生し、第 4 の受信装置 154 で 1 回再生するものとする。第 1 の権利情報及び第 3 の権利情報 153 は各々表 30、表 31 となる。表 31 では第 9 の受信装置 320 で 1 回再生しているので再生回数を 1 回減じている。

【0148】

【表 30】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【 0 1 4 9 】

【表 3 1】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【 0 1 5 0 】

その他の動作は本発明の第 5 の実施の形態と同様である。これによって、第 9 の受信装置 3 2 0 は、受信した権利情報、ビットストリーム、ツール情報等を第 4 の受信装置 1 5 4 に送ることが可能となる。

【 0 1 5 1 】

(第 1 1 の実施の形態)

図 1 4 は、本発明の第 1 1 の実施の形態における受信装置を示すブロック図である。本発明の第 1 1 の実施の形態は第 1 の送信装置 7 3 と第 2 の受信装置 1 3 0 と第 2 の受信装置にネットワークによって接続された第 1 0 の受信装置 1 4 4 に関するものである。図 1 4 において、4 9、5 0 は図 1 5 に示す従来例の構成と同様であり、6 6、7 3、7 4 は図 1 に示す本発明の第 1 の実施の形態と同様であり、1 1 1、1 1 4、1 3 0、1 3 6、1 4 0、1 4 3、1 4 4 は図 5 に示す本発明の第 4 の実施の形態と同様である。

【 0 1 5 2 】

図 1 4 にて、第 1 0 の受信装置 1 4 4 は第 2 の要求情報 1 4 0 を第 2 の受信装置 1 3 0 に出力する。第 2 の受信装置 1 3 0 は状態情報 7 4 を第 1 の送信装置 7 3 に出力する。第 1 の送信装置 7 3 は、本発明の第 1 の実施の形態と同様に第 1 の多重化ビットストリーム 6 6 を出力する。第 2 の受信装置 1 3 0 が受信する第 1 の多重化ビットストリーム 6 6 は本発明の第 4 の実施の形態では 1 0 1 と記されており、本発明の第 4 の実施の形態と同様に処理されてビデオ復号手段 1 1 1 とデジタルオーディオ信号 1 1 4 を出力すると共に第 2 の多重化ビットストリーム 1 4 3 として第 1 0 の受信装置 1 4 4 に出力される。第 1 0 の受信装置 1 4 4 は、本発明の第 3 の実施の形態と同様に動作し、第 2 の返信情報 1 3 6 を出力する。

【 0 1 5 3 】

【発明の効果】

以上説明したところから明らかなように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供することのできる信頼性の高い送信装置を提供することができる。

【 0 1 5 4 】

また、本発明は、上記効果に加えて、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報のプログラム仕様情報の一部として処理することができるという利便性を提供することができる。

【 0 1 5 5 】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を有する送信装置を提供することができる。

【 0 1 5 6 】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【 0 1 5 7 】

また、本発明は、上記効果に加えて、暗号を復号する復号ツールも同時に多重化して送信する利便性を有する送信装置を提供することができる。

【 0 1 5 8 】

また、本発明は、上記効果に加えて、暗号を復号するための鍵情報も同時に多重化して送信する利便性を有する送信装置を提供することができる。

【 0 1 5 9 】

本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部としてダウンロードすることができるので更新可能であり、常に最新の保護方式を組み込むことができる信頼性の高い受信装置を提供することができる。

【 0 1 6 0 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することが可能であるばかりでなく、多重化情報のプログラム仕様情報の一部として処理できる利便性を有する受信装置を提供することができる。

【 0 1 6 1 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することができるばかりでなく、権利情報を上記多重化情報とは別のファイルで受信することができるので権利情報を多重化情報とは別に扱うことができるという利便性と別の受信装置に転送する場合の任意性を与えることができる受信装置を提供することができる。

【 0 1 6 2 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、権利情報に基づいて受信した暗号化データを消去することができるので使用済みのコンテンツを受信装置に残すことがなく不正な使用を防止することができる信頼性の高い受信装置を提供することができる。

【 0 1 6 3 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供する受信装

置を提供することができる。

【 0 1 6 4 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報を別の受信装置にダウンロードすることができるので更新可能であり、常に最新の保護方式を維持できることに加えて、別の受信装置が受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供し受信装置を提供することができる。

【 0 1 6 5 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した権利情報を分割して別の受信装置に暗号化データとともに送信することができるので別の受信装置でも同様に暗号化データを高信頼性のもとに処理することのできる受信装置を提供することができる。

【 0 1 6 6 】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信装置が受信したデータを変換することにより別の受信装置に最適な信号として転送することが可能な受信装置を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態における送信装置の概略構成を示す図

【図 2】

本発明の第 1 の実施の形態における制御グラフ

【図 3】

本発明の第 2 の実施の形態における送信装置の概略構成を示す図

【図 4】

本発明の第 3 の実施の形態における受信装置の概略構成を示す図

【図 5】

本発明の第 4 の実施の形態における受信装置の概略構成を示す図

【図 6】

本発明の第 4 の実施の形態における第 2 の権利管理手段の概略処理を示す図

【図 7】

本発明の第 4 の実施の形態における多重化ビットストリームの概略構成を示す図

【図 8】

本発明の第 5 の実施の形態における受信装置の概略構成を示す図

【図 9】

本発明の第 6 の実施の形態における受信装置の概略構成を示す図

【図 1 0】

本発明の第 7 の実施の形態における受信装置の概略構成を示す図

【図 1 1】

本発明の第 8 の実施の形態における受信装置の概略構成を示す図

【図 1 2】

本発明の第 9 の実施の形態における受信装置の概略構成を示す図

【図 1 3】

本発明の第 1 0 の実施の形態における受信装置の概略構成を示す図

【図 1 4】

本発明の第 1 1 の実施の形態におけるシステム構成を示す図

【図 1 5】

従来 of 構成図

【符号 of 説明】

5 1 権利情報生成手段

5 3 制御グラフ生成手段

5 4 制御情報生成手段

6 0 暗号化手段

6 3 暗号化ビデオビットストリーム

- 7 3 第 1 の送信装置
- 7 4 状態情報
- 8 5 送信権利情報
- 9 0 読み出し情報
- 9 5 ツールリスト分離手段
- 9 7 権利情報分離手段
- 1 0 1 第 1 の多重化ビットストリーム
- 1 0 8 組み込み手段
- 1 1 5 復号ツール
- 1 2 0 第 1 の制御手段
- 1 2 1 第 1 の権利管理手段
- 1 2 4 ファイル管理手段
- 1 3 2 第 1 の返信情報
- 1 3 3 第 2 の権利情報
- 1 3 6 第 2 の返信情報
- 1 3 7 第 1 の要求情報
- 1 3 8 第 2 の権利管理手段
- 1 3 9 第 2 の制御手段
- 1 4 0 第 2 の要求情報
- 1 4 1 第 1 の制御情報
- 1 4 3 第 2 の多重化ビットストリーム
- 1 5 3 第 3 の権利情報
- 1 6 0 第 3 の制御手段
- 1 6 1 第 3 の権利管理手段
- 2 3 1 第 4 の制御手段
- 2 3 2 第 4 の権利管理手段
- 2 5 1 第 5 の権利管理手段
- 2 5 2 第 5 の制御手段
- 2 5 4 第 2 の暗号化ビデオビットストリーム

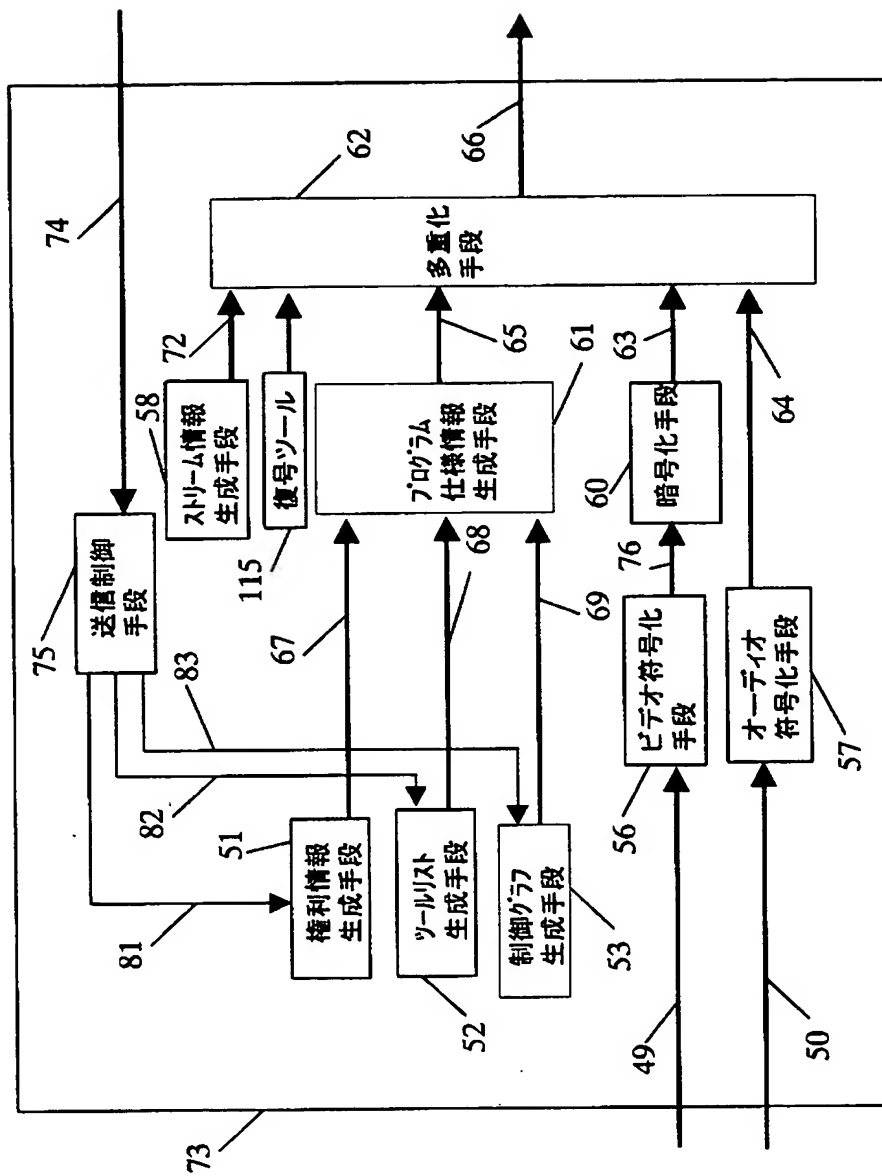
2 5 5 再多重化手段

2 5 6 第 3 の多重化ビットストリーム

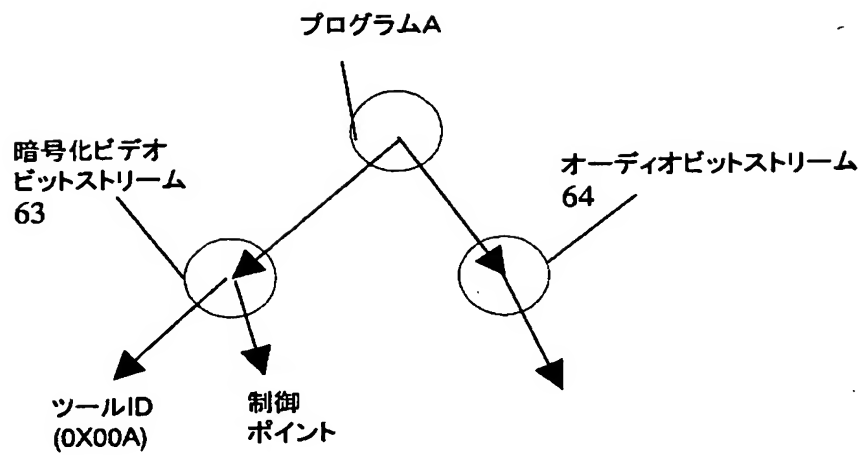
2 5 8 第 3 の要求情報

【書類名】 図面

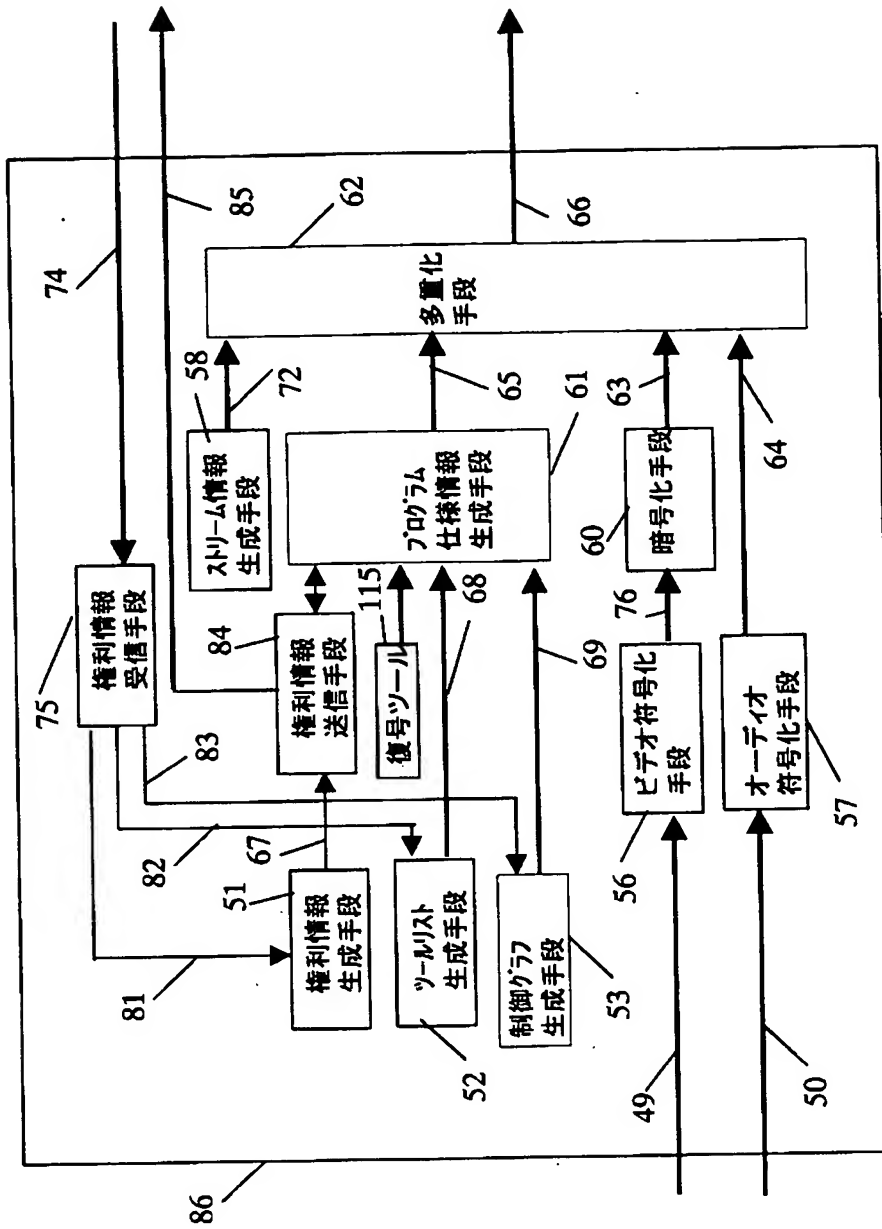
【図1】



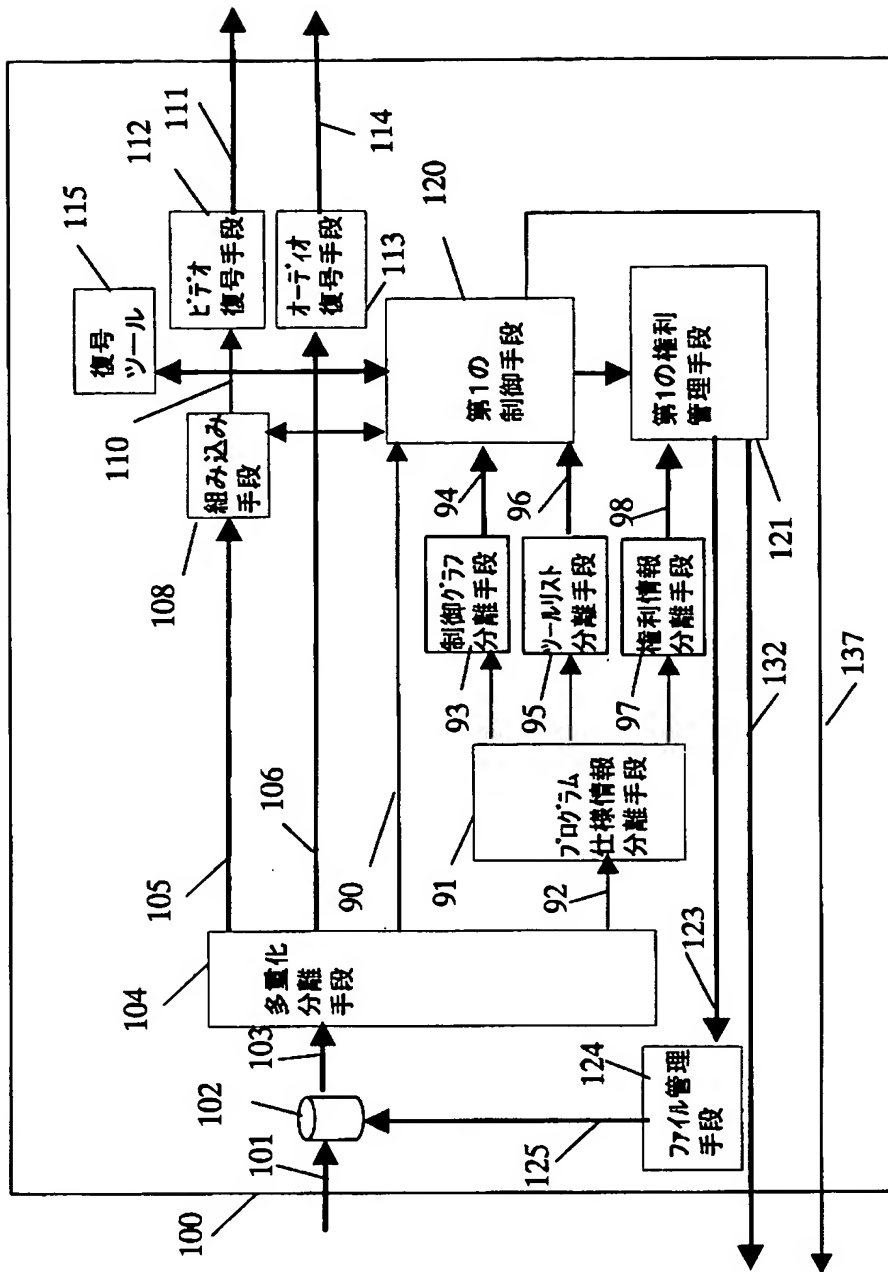
【図 2】



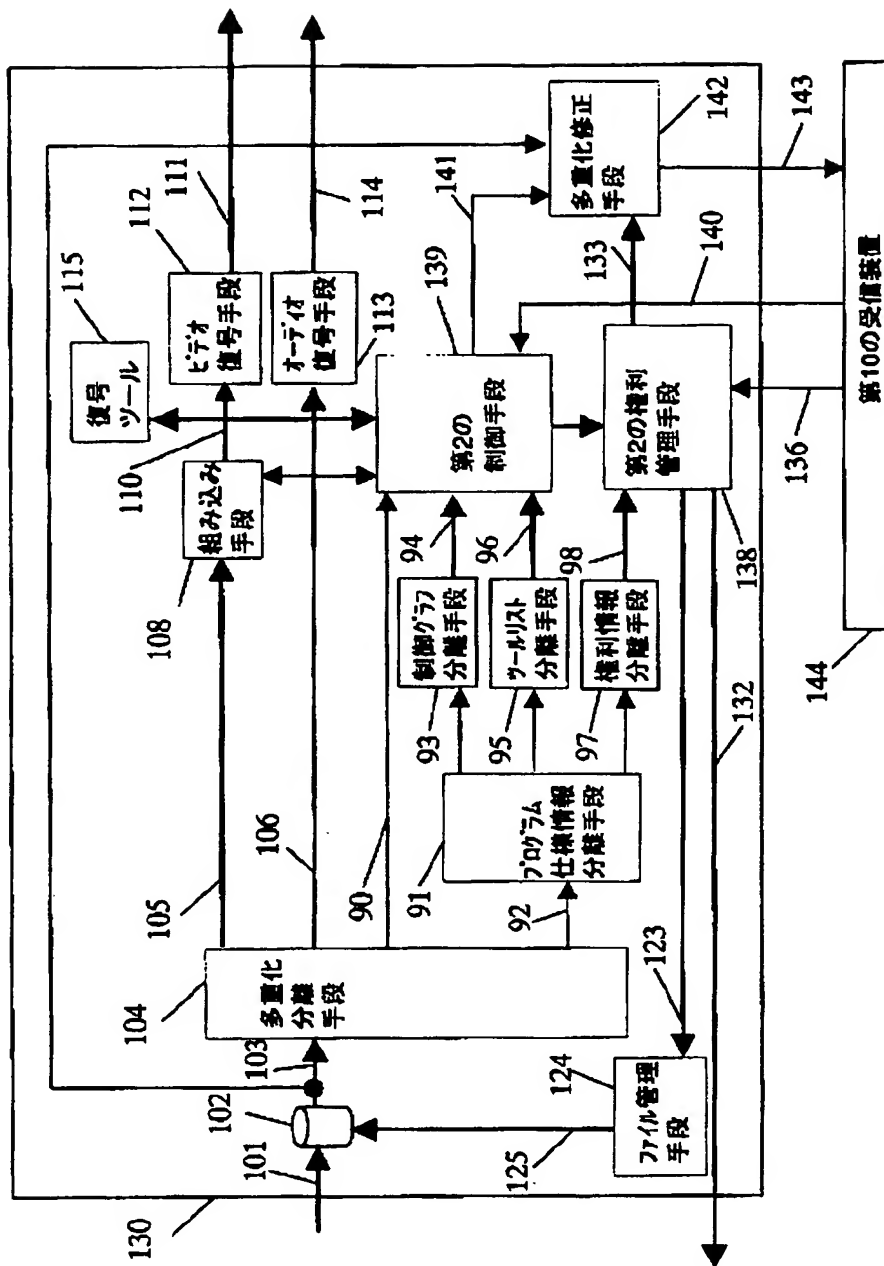
【図3】



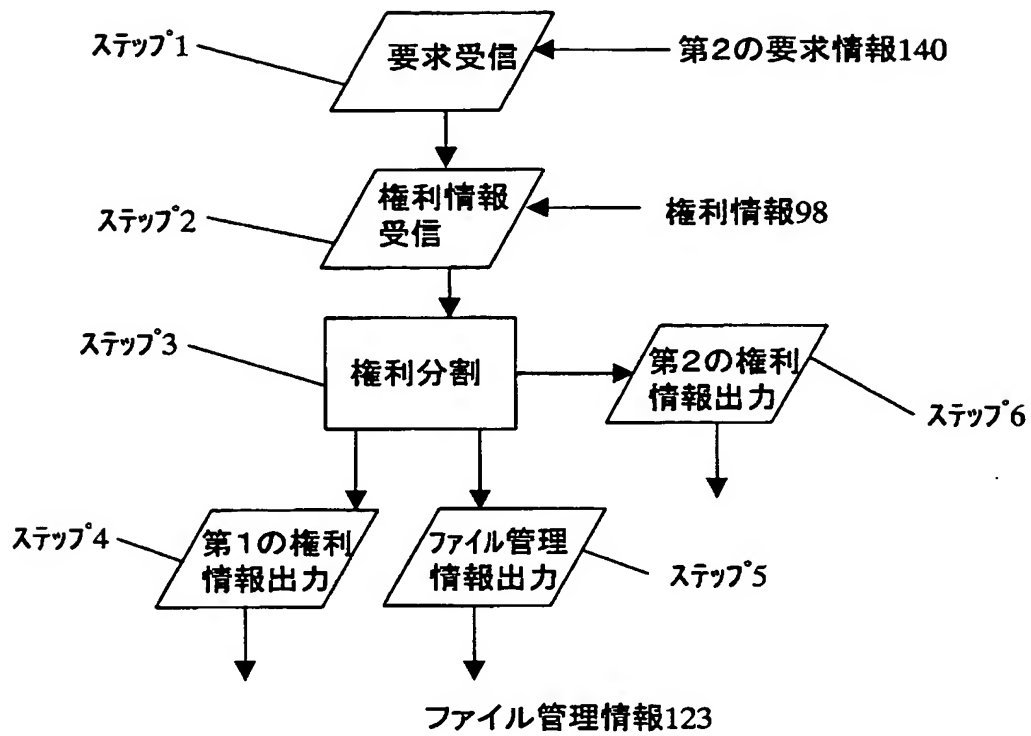
【図 4】



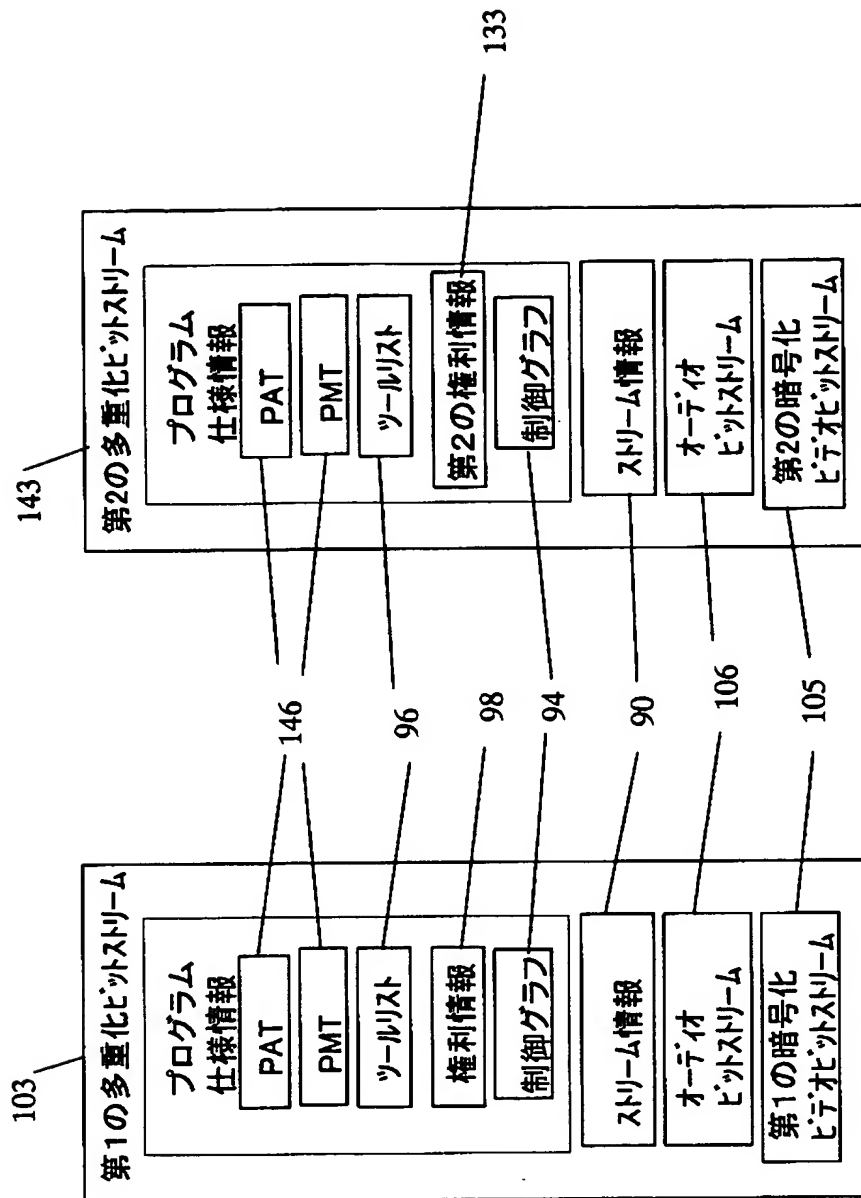
【図5】



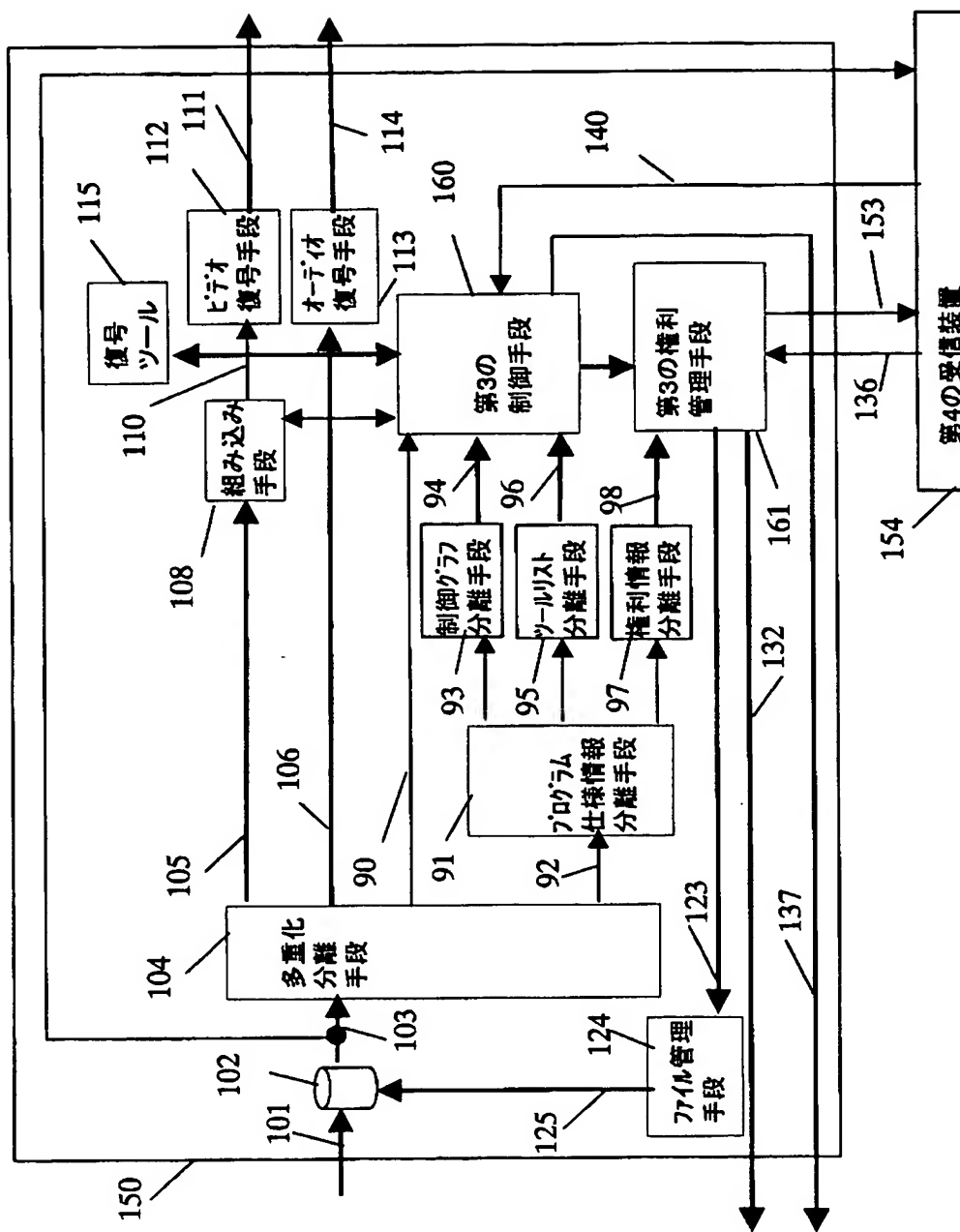
【図 6】



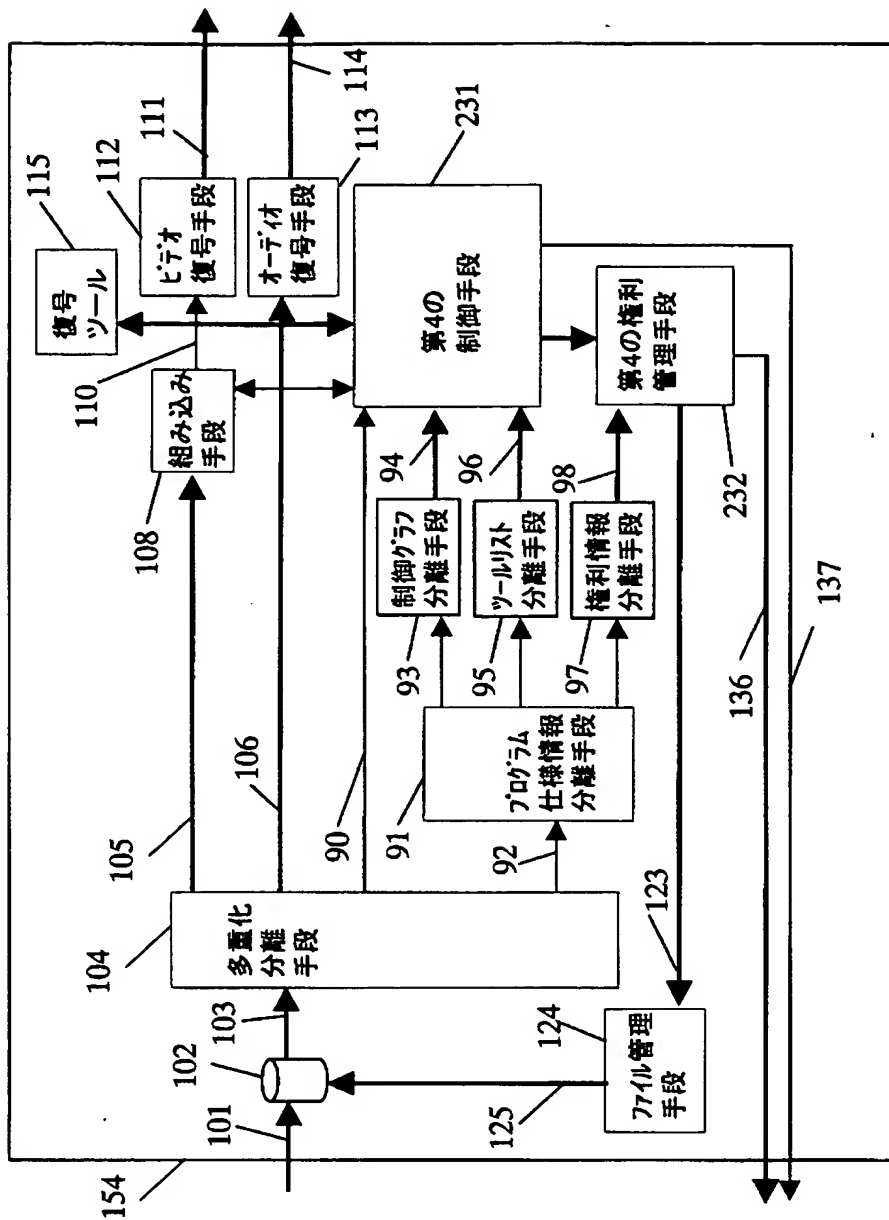
【図7】



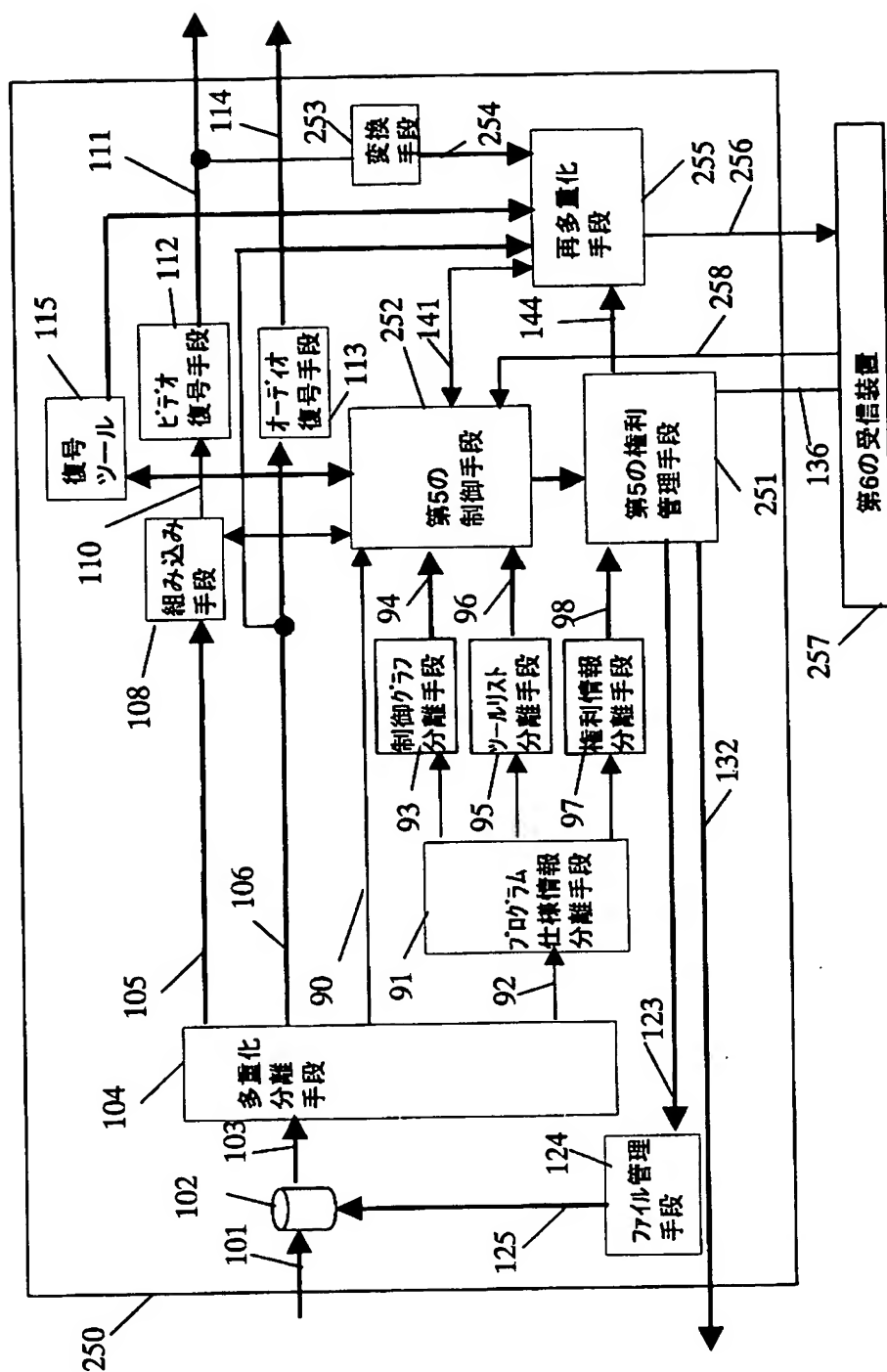
【図 8】



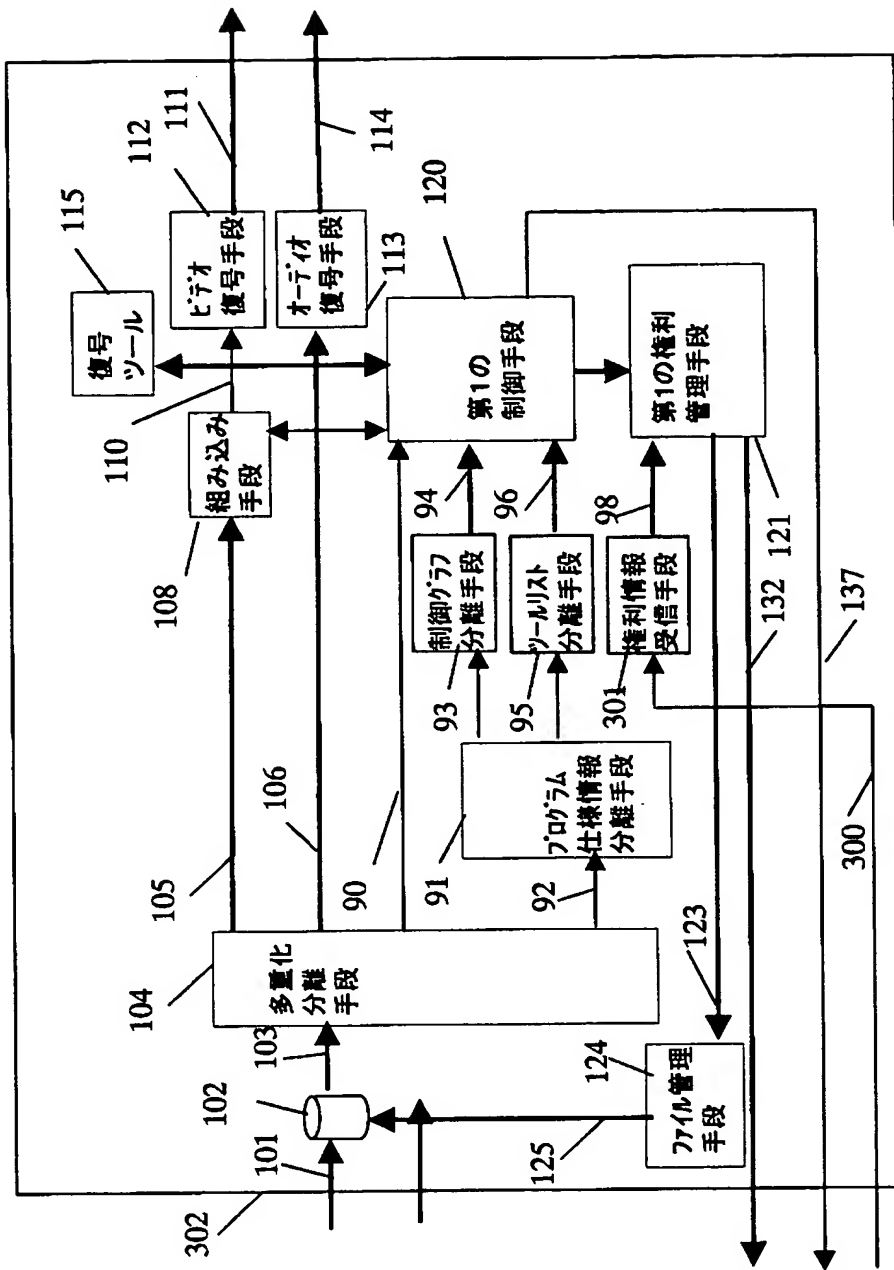
【図9】



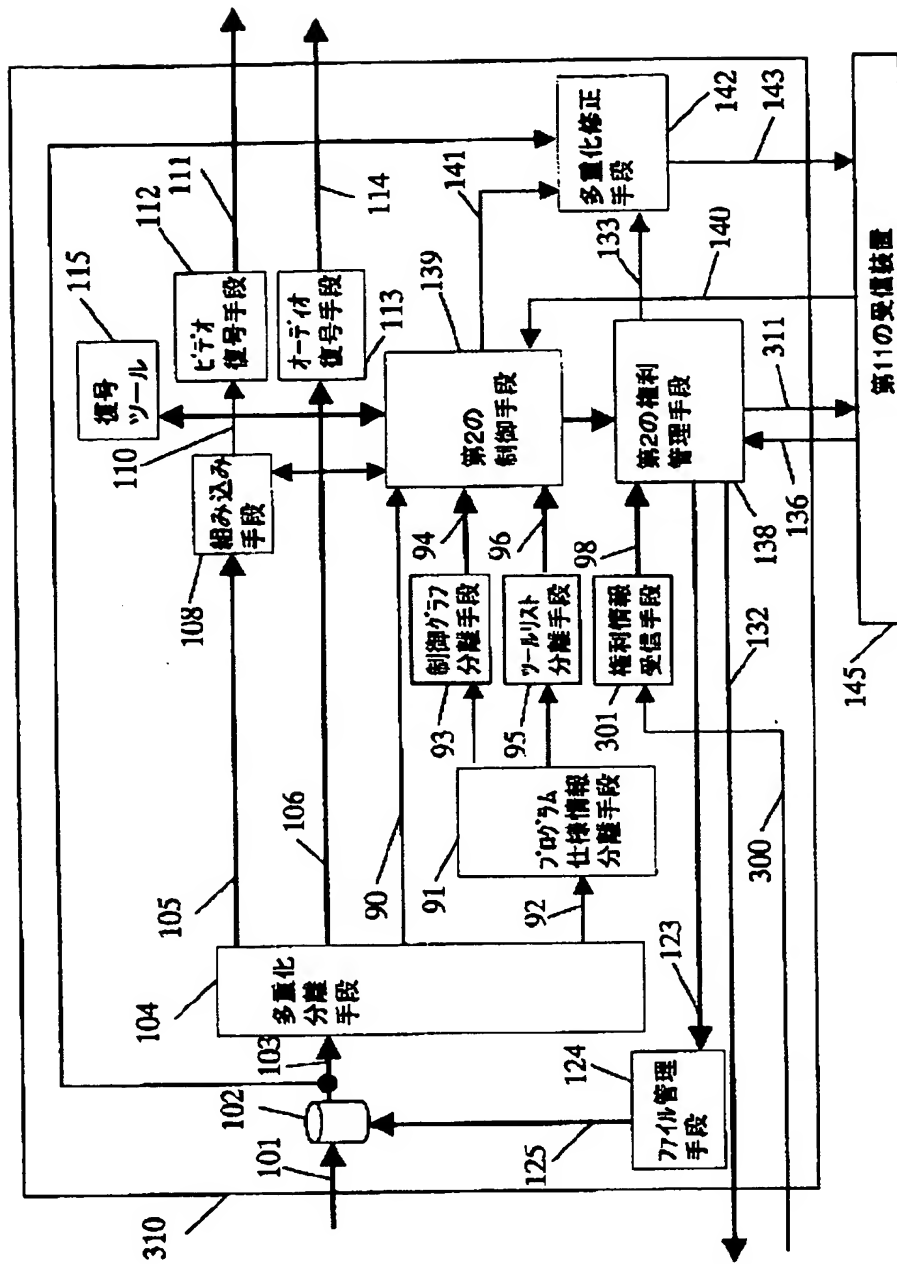
【図10】



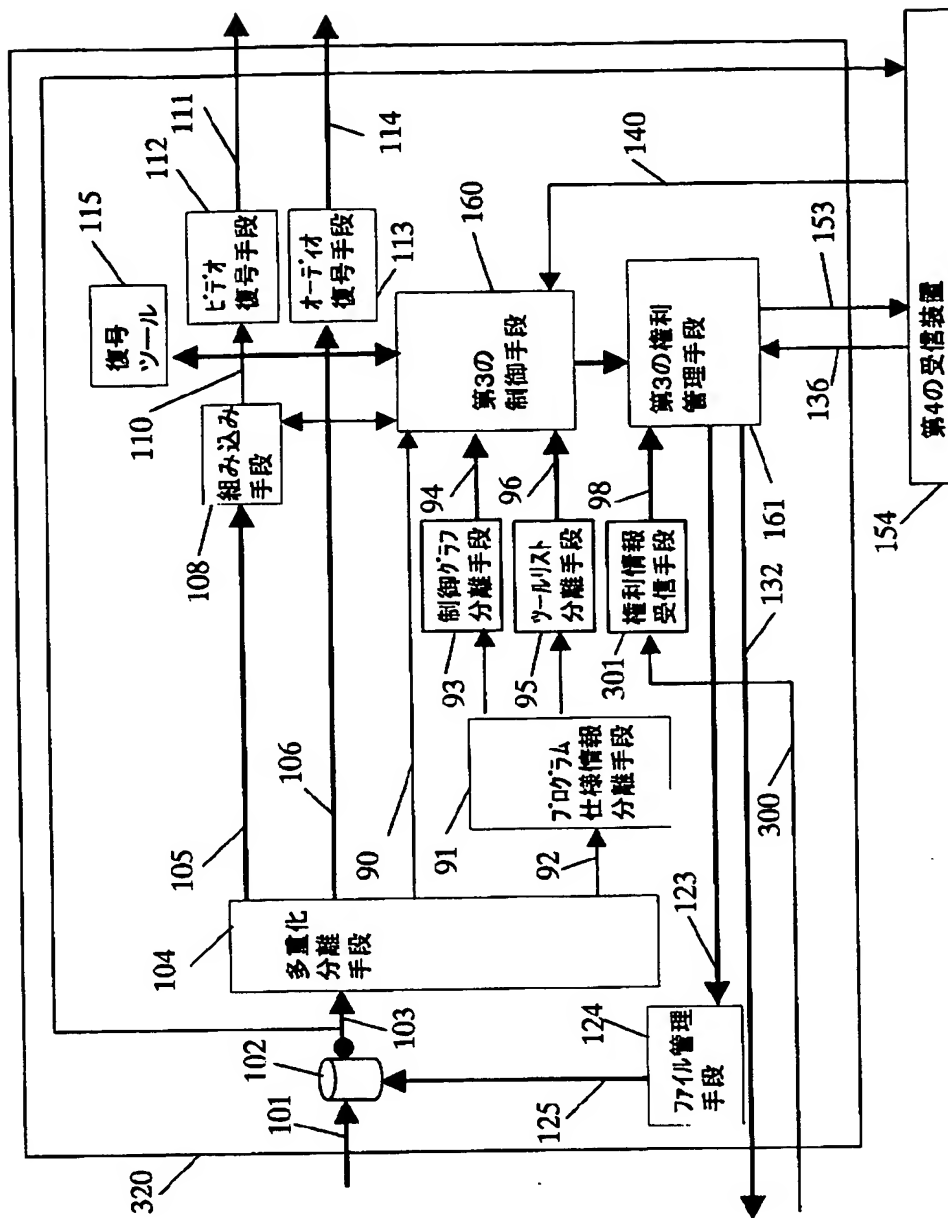
【図 11】



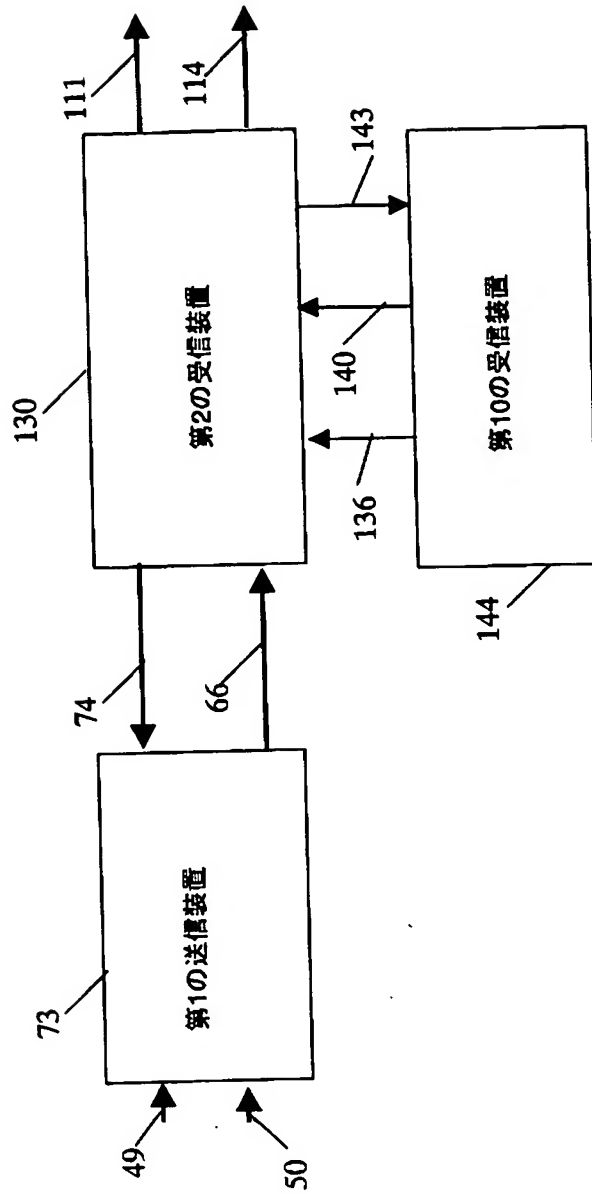
【图 12】



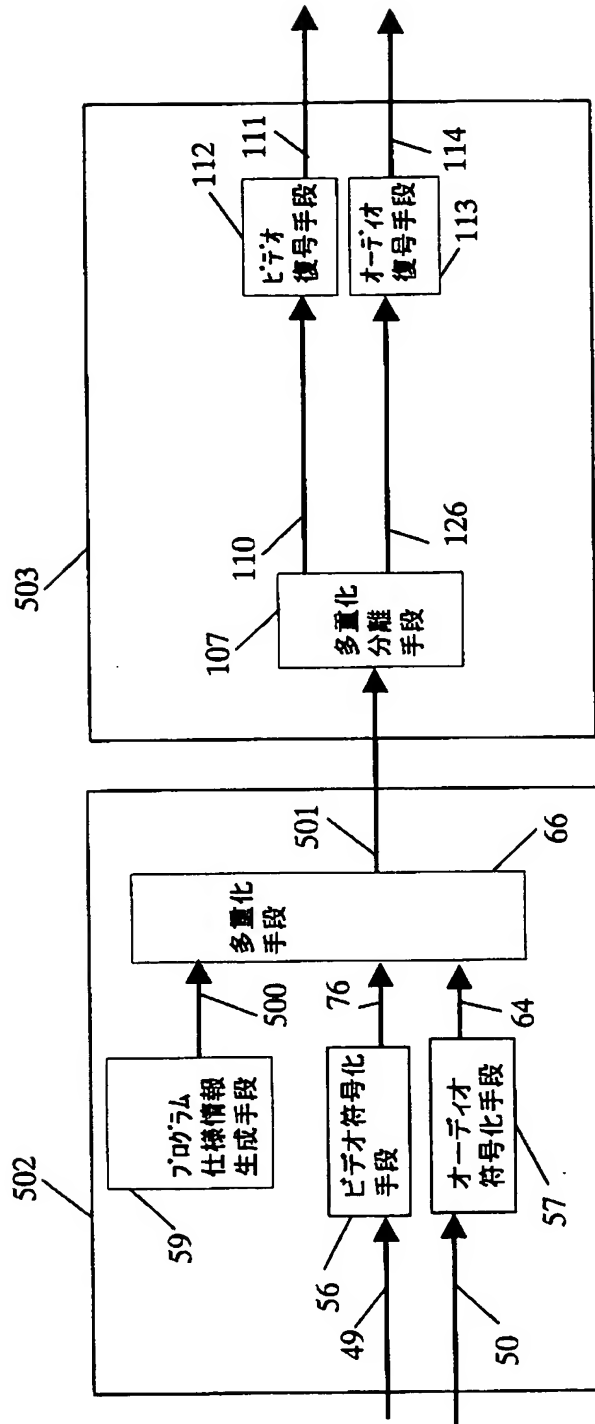
【图 1 3】



【図14】



【図 15】



【書類名】 要約書

【要約】

【課題】 暗号化の仕組みを破られた場合に、暗号化の仕組みを更新する送受信装置を提供すること。

【解決手段】 暗号化データの復号ツールのツールIDを取得、存在の確認とツールの取得、更新を行うとともに、上記暗号化データに付随する権利情報に基づいて上記暗号化データの処理と転送を行う。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社